My Data My Privacy My Choice

A Step-By-Step Guide to Secure your Personal Data and Reclaim your Online Privacy!

ROHIT SRIVASTWA

bpb

My Data My Privacy

My Choice

A Step-by-Step Guide to Secure Your Personal

Data and Reclaim Your Online Privacy!

---

by

Rohit Srivastwa

FIRST EDITION 2020

ISBN: 978-93-89845-181

Distributors:

BPB PUBLICATIONS

20, Ansari Road, Darya Ganj

New Delhi-110002

Ph: 23254990/23254991

MICRO MEDIA

Shop No. 5, Mahendra Chambers,

150 DN Rd. Next to Capital Cinema,

V.T. (C.S.T.) Station, MUMBAI-400 001

Ph: 22078296/22078297

DECCAN AGENCIES

4-3-329, Bank Street,

Hyderabad-500195

Ph: 24756967/24756400

BPB BOOK CENTRE

376 Old Lajpat Rai Market,

Delhi-110006

Ph: 23861747

Published by Manish Jain for BPB Publications, 20 Ansari Road, Darya Ganj, New Delhi-110002 and Printed by him at Repro India Ltd, Mumbai

Dedicated to

Everyone who respects their privacy and wants to live a safe life online

Foreword

The COVID-19 pandemic has made “virtual,” the new reality, and we are now living in an age where the internet is no longer a novelty but a necessity. What began as a rather complicated way to send simple messages from one machine to another has now evolved into a behemoth that allows us to do all kinds of things – simple AND complicated – often, at the mere touch of a button. We have rapidly progressed from sending each other little packets of text to doing almost everything – communicating, shopping, relaxing, creating, sharing, spreading – on the internet.

However, this evolution has extracted a high cost from us. Every username and password combination that we create on the internet is a tiny peephole into our lives. The notion of privacy exists only as long as these peepholes remain unknown to outsiders. The more peepholes we create, the more vulnerable we make ourselves to all these outsiders, who will relish any opportunity to sneak a free peek into our lives.

Consider this, the website “Have I Been Pwned” (https://haveibeenpwned.com) contains a record of more than 9.5 billion accounts from 440 websites that were ‘hacked’ by miscreants. DeHashed (https://www.dehashed.com) contains 12.5 billion “compromised assets” from “all corners of the internet.”

There is a genuine chance that one of those accounts could belong to you. If you are the kind of person who reuses their password across multiple websites and doesn’t change passwords very often, then all your accounts are suddenly open to invasion. From merely having one leaked account, your entire online presence suddenly went under threat.

The early users of the internet merely had to contend with fundamental problems such as transmission and display of data. Today, the average internet user transmits several pieces of PII – personally identifiable information – to remote servers, often without realizing it. Were this information to get leaked or intercepted, it could represent a significant threat to our well-being. The need to ensure the security of our online identities and the privacy of our online data should, therefore, be considered paramount in this day and age.

That’s where Rohit Srivastwa’s years of expertise with cyber-security and digital privacy comes in handy. With his book, “My Data, My Privacy, My Choice,” Rohit offers a clear and well-laid path to extricate yourself out of the mess that is maintaining the privacy of your online identities.

Rohit guides you, the reader, carefully, with step-by-step instructions that take you from understanding the problem to solving the problem. The solutions (wonderfully named #RohitRecommends) are structured carefully in a four-tiered structure ranging from Basic to Expert, with each subsequent level providing a stronger layer of security and better privacy for your online identity. Each level of recommendation is self-sufficient (to a degree), and there is no compulsion to follow recommendations at a level that you find difficult to comprehend.

Rohit has also introduced a gamification framework to incentivize the adoption of these recommendations by assigning ‘points’ to each recommended action. As you go through the book, you collect points, and the final tally gives you an idea of your PrivacyScore. The higher the level of recommendations followed, the better your PrivacyScore will be.

Another unique aspect of the book is its interactive, cross-media capabilities. Instead of relegating relevant reading to the usual ‘References’ section, the book uses smartly-placed, contextual QR codes that you can scan to acquire additional knowledge of the subject without ever leaving the page of the book that you are on!

Rohit Srivastwa strives to make the subject of online privacy and cybersecurity easy to understand and implement for everyone. He has succeeded in creating a framework that makes it easy for everyone to implement a degree of control over their online data and reclaim their online privacy.

Lt. Gen Rajesh Pant, PVSM, AVSM, VSM (Retd.), PhD

National Cyber Security Coordinator - PMO

Govt of India, New Delhi

Testimonials

The thing about the internet is that it is a wonderful place, BUT there are some not-so-wonderful people on it…

“My Data, My Privacy, My Choice!” by Rohit Srivastwa makes it easy to explore the wonders of the internet while ensuring that you avoid bumping into these not-so-wonderful people! I felt that the gamification of recommended actions (#RohitRecommends) ensured that I, as the reader, was substantially incentivized actually to follow the recommendations set out. By the end of the book, I could see a clear difference in my browsing habits, and I could *feel* my network traffic heaving a sigh of relief!

Rohit Srivastwa has written a superb guide with valuable information on every page written in easy-to-understand language. I highly recommend it for those who are looking to get started on the journey to securing their online identity and reclaiming the privacy of their digital data

- Brijesh Singh, IPS

Former Inspector General of Maharashtra Cyber

As our physical and digital world merge, we need to go in for certain lifestyle changes so as to protect ourselves from digital threats and safeguard our privacy continuously as technology shapes our every-day lives. While various learning platforms, scholarly articles on the internet, online courses, watching Youtube, podcasts, blogs, etc. can help create awareness and learning amongst us, however, it is an excellent book that is the best way to get in-depth knowledge which is the most helpful. With years of experience in the cybersecurity and privacy domain, Rohit Srivastwa, as a first-time author, has shared his in-depth knowledge in a clean, understandable, lucid, and practical manner. Rohit has cleverly weaved the concepts of gamification with the educational objective of making awareness and learning more appealing while motivating users by providing insightful suggestions neatly categorized into basic, intermediate, advanced, and expert - thus nudging you to improve your baseline continuously.

Pick up “My Data, My Privacy, My Choice” and take action today so that you can embark upon your digital adventure confidently and enjoy your journey!

- Dr. Sanjay Bahl, Director General

Indian Computer Emergency Response Team (CERT-In)

About the Author

Rohit Srivastwa is a serial entrepreneur, a recipient of Microsoft MVP award in the domain of “Enterprise Security,” and a multifaceted professional with experience in Cyber Security, Enterprise Security, Enterprise IT, Secure Digital Transformation and Cyberwarfare. He is also actively involved in advising several Military agencies, Law Enforcement, Corporate, and Government bodies of different countries in these fields.

He is a well-known Security Evangelist and Founder of India’s first-ever hackers’ conference and community named “ClubHack.” He has had a bunch of start-ups in the past, with the last one acquired by QuickHeal Technology Ltd in 2016.

A teacher at heart, Rohit has designed the entire MTech program in Information Security that is being currently offered by Pune University. He is also a visiting faculty at several A-grade institutions such as IITs, IIMs, Symbiosis, etc. He is a liaison member at FIRST.org, where his responsibilities include liaising between CERTs of different countries and companies.

He has been featured in many technical shows and news panel discussion related to cyber warfare and cybersecurity. Rohit is also a renowned speaker and has spoken in many events across the globe, including TEDx, Microsoft Digital Crime Convention, among others.

Current Roles

Founder, ClubHack Labs

Virtual CISO, Various Large enterprises

Advisor, Science & Technology Park, Dept of Science & Technology, Govt of India

Mentor and Advisor, Several Cyber Security Start-ups

Charter Member, TiE

You can tweet the author @rohit11 and also follow his security and privacy recommendations on twitter using #RohitRecommends

Acknowledgement

This book would not have been possible without the unwavering support of my family, specifically, my lovely wife, Stuti, and my sons. I know I have missed a few important moments over these last several months, but I promise I'll make it up to you soon!

To my mentors in the industry whose work has inspired me to write this book, I owe you a debt of gratitude. To the people who helped me along the way, I owe you a ton of thanks.

To the people who lurked in the shadows and were always ever an email or a phone call away whenever I needed them – thank you for being available at a moment's notice! I couldn't have written this book without you!

Finally, thank you BPB for giving a first-time author this opportunity to write his first book. Thank you for believing in me, in this book, and in the crazy ideas that I kept pitching through the process. You guys are total rockstars!

Preface

"Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively."

- Wikipedia

Privacy means ensuring that you are able to hide your actions from people who want to snoop on you. Privacy means ensuring that things you do not want to share with the rest of the world do not get shared with the rest of the world. Privacy means being able to choose what others get to know about you. Privacy means having the ability (and the right) to keep certain information -- such as your email credentials, banking credentials, whether or not you like sushi -- completely secret.

Your personal information belongs to you and you alone. It should never ever be available for anyone else to see without your knowledge and without your explicit permission.

Over the last few years, with free/cheap data packs becoming abundantly available more and more Indians have been able to witness the glory of this wonderful innovation called the Internet. Combine them with cheap smartphones, and almost every person on the street seems to be glued to some streaming service or the other.

The Internet, however, is not like any other mode of entertainment - it takes as much as it gives, sometimes more than that. Each time you open an app, each time you click a link, you are conveying a choice, a selection, a conscious effort on your part, and someone somewhere is tracking it all. Every choice your make is being silently recorded. Every page you view is being silently analyzed. Every habit you form is being silently judged.

Moreover, things that you do online are never forgotten; they are remembered for eternity. Anything you post online -- be it a photo, or a video, or audio, etc. -- everything that you share remains on the interwebs forever and ever.

In this book, I argue that privacy is as much a fundamental right as the right to life. In fact, the argument for privacy can be made in the same vein as the example of "The Truman Show" i.e., we need privacy, not because we have something to hide, but because someone else does not get to decide whether or not it is right for us.

This book will help you understand how much of your personal information gets freely shared on the internet without your explicit knowledge and authorization. This book will also give specific and comprehensive instructions on how you can take control of all that information.

By the end of this book, you will have ensured that the information being leaked by your phone, your desktop, your browser, and your internet connection is minimal-to-none. All your online accounts for email, social networks, banking, shopping, etc. will be secure and (significantly) impervious to attackers. You will have complete control over all of your personal information that is available to public view. In fact, if you so choose, you will even be able to create 'purposeful misinformation' to counter any potential threats to your privacy and security, if and when necessary.

Over the 15 chapters in this book, you will learn the following:

Chapter 1 introduces a quick self-assessment and establishes some 'ground-rules' by defining various terms and concepts such as #RohitRecommends and the scoring system used throughout this book.

Chapter 2 explains how various devices, services, and adversaries of all kinds have the potential to track and extract your private information by outlining basic and advanced methods to proactively identify leakage of personal information.

Chapter 3 discusses the Android operating system, explores the privacy concerns surrounding them, and provides recommendations on how to

deal with such issues.

Chapter 4 looks at the various Apple devices available in the market, attempts to understand the privacy concerns surrounding them and provides recommendations on how to deal with such issues.

Chapter 5 highlights the various issues with the app-ecosystem present in both the mobile platforms – Android and iOS – and provides recommendations on how to identify and deal with such apps.

Chapter 6 explores various 'smart' devices available in the market and how they can impact the privacy of your personal data and provides specific recommendations on how to ensure the privacy of your personal data while using smart devices and/or IoT.

Chapter 7 evaluates how known vulnerabilities in popular desktop operating systems can be exploited by malicious actors to prey on your personal data and provides recommendations on how to deal with these vulnerabilities/exploits.

Chapter 8 evaluates how commonly exploited vulnerabilities in software applications can be exploited by malicious actors to prey on your personal data and provides recommendations on how to deal with these vulnerabilities/exploits.

Chapter 9 evaluates commonly used desktop browsers, discusses how they can be exploited by malicious actors to prey on your personal data, and provides recommendations on how to deal with these vulnerabilities/exploits.

Chapter 10 explores the privacy issues and threats associated with accessing email, how it can be compromised by malicious actors, and provides recommendations to secure your email inbox.

Chapter 11 evaluates different categories of software provided as services (a.k.a. SaaS) over the internet, i.e., Social Networks, Netbanking, Shopping websites, etc. and the privacy issues and threats to consider while accessing these services over the internet.

Chapter 12 discusses the various methods of connecting to different networks (such as Broadband, Wi-Fi, GSM/CDMA, Bluetooth, NFC, etc.) and evaluates each of them from a privacy perspective.

Chapter 13 discusses Operational Security (OPSEC) and presents simple Dos and Don'ts that you can follow to implement OPSEC-like behaviors in your daily routines.

Chapter 14 summarizes all the learning from the previous chapters and invites you to re-assess yourself. If you did everything right up to this point, you should be able to see significant improvement over the results you received in the first chapter!

Chapter 15 contains information that is important to know but a little too detailed for casual reading. You can skip this chapter if you'd like, but I strongly recommend you read it anyway.

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors if any, occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Table of Contents

Section 1: Introduction

1. Prologue

Introduction

Before we begin…

Who should read this book?

How to read this book?

What is #Rohit Recommends?

Basic

Intermediate

Advanced

Expert

The points system

Conclusion

1. Internet and Privacy

Introduction

Privacy? What privacy?!

Google

Microsoft

Facebook

Cambridge Analytica

Adversaries and threats

Passive adversaries

Active adversaries

Intrusive advertising

Invisible threats

What we already know about you

The basics of snooping

Advanced snooping or OSINT

Conclusion

Section 2: Devices

1. Android Devices

Introduction

The Google-Android ecosystem

Android Open-Source Project (AOSP)

So, why does Google do this?

What is a ROM?

Official ROMs

Custom ROMs

Official firmware vs custom ROMs

Android and privacy

Google Telemetry

Non-Google Telemetry

OnePlus Telemetry

Xiaomi Telemetry anddata breach

…and others!

Recommendations and suggestions

Sensors

Permissions

RohitRecommends

Google Telemetry

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

EXPERT: (5 points)

Non-Google Telemetry

BASIC: (1 point)

Sensors

BASIC: (1 point)

Permissions

BASIC: (1 point)

INTERMEDIATE: (2 points)

Conclusion

1. Apple iPhones

Introduction

The Apple Ecosystem

iOS

iCloud

Jailbreaking

Apple and Privacy

Sensors

Permissions

The Settings App

Analytics and Advertising

RohitRecommends

iOS and iCloud

BASIC (1 point)

ADVANCED (3 points)

Sensors

BASIC (1 point)

ADVANCED (3 points)

Permissions

BASIC (1 point)

ADVANCED (3 points)

Settings | Privacy

BASIC (1 point)

Analytics and Advertising

BASIC (1 point)

INTERMEDIATE (2 points)

Conclusion

1. Smartphone Apps

Introduction

Bloatware

How to Identify Bloatware on Android?

Malware

What are the Different Kinds of Malware?

How Do I Know I'm Affected?

Why Doesn't Someone Do Something, Then?

How can I prevent malware attacks in the future?

Sandboxing

Permissions

RohitRecommends

Bloatware

On Android

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

EXPERT: (5 points)

Malware

BASIC: (1 point)

ADVANCED: (3 points)

Sandboxing

BASIC: (1 point)

Permissions

BASIC: (1 points)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

Conclusion

1. Smart Devices and IoT

Introduction

The Internet of Things (IoT)

Security vulnerabilities in IoT and smart devices

Strava

Smart TVs

Alexa, Siri, and Google

Smart appliances

RohitRecommends

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

EXPERT: (5 points)

Conclusion

1. Desktops Operating Systems

Introduction

Operating systems

Microsoft Windows

Modern Windows (Win10, Win 8.1, and Win8)

Windows 7 and older versions

macOS

Linux

Multi-OS systems

Dual boot

Virtual machines

Live OS

Data persistence

Default user: administrator vsguest

Telemetry

Windows 10 telemetry

Diagnostics and feedback

Keystroke logging

Cortana

Wi-Fi Sense

Apple’s Keychain and ‘KeySteal’

Other privacy settings

RohitRecommends

Operating system (OS)

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

EXPERT: (5 points)

Spy vs Spy!

Telemetry

Diagnostics & feedback

Keystroke logging

Cortana

Wi-Fi Sense

Other ‘Privacy’ Settings

BASIC: (1 point)

INTERMEDIATE: (2 points)

macOS

BASIC (1 point)

INTERMEDIATE (2 points)

EXPERT (5 points)

Linux

BASIC (1 point)

ADVANCED (3 points)

Conclusion

1. Desktops-Software Applications

Introduction

Software applications

Bloatware

Manufacturer-branded utilities

Third-party apps and utilities

Integrated Bloatware

Security software

Firewalls

Antivirus and anti-malware

RohitRecommends

Software applications

BASIC (1 point)

INTERMEDIATE (2 points)

ADVANCED (3 points)

Sandboxing

File encryption

System restore

Bloatware removal

Windows 10

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED (3 points)

EXPERT (5 points)

Apple (macOS)

BASIC: (1 point)

Linux

BASIC: (1 point)

Security software

Windows 10

Firewalls

BASIC: (1 point)

INTERMEDIATE: (2 points)

Antivirus & Anti-malware

BASIC: (1 point)

INTERMEDIATE: (2 points)

macOSand Linux

BASIC: (1 point)

Antivirus andanti-malware

ADVANCED (3 points)

Antivirus and anti-malware

Conclusion

1. Desktops-Browsers

Introduction

How do modern browsers work?

Popular browsers

Privacy-aware browsers

Brave browser

Epic browser

The Tor browser

Is Tor truly anonymous?

Privacy settings

Private windows

Telemetry opt-out

Syncing and personalization

Search engine integration

Cookies, tracking, and content blocking

Forms and autofill

Permissions andsite settings

Plugins and extensions

The difference

Plugins and extensions are fundamentally different

Potential security concerns with plugins

Potential security concerns with extensions

RohitRecommends

BASIC (5 points)

Browser recommendation

Private browsing

Privacy settings

Extensions

INTERMEDIATE: (10 points)

ADVANCED: (15 points)

Browser recommendation

Private browsing

Privacy settings

Extensions

EXPERT: (25 points)

Installing Tor

Using Tor

Caveat Emp-tor!

Conclusion

1. Services - Email

Introduction

Email

Accessing email

Web-based portals

Email clients

Compromising your email

Phishing

Weak passwords

Malware

Email ads

Hosting your own email server

Using a privacy-aware email service provider

Spam

RohitRecommends

Accessing your email

Web-based portals (BASIC, 1 point)

Offline clients (BASIC, 1 point)

Compromising your email

Phishing

BASIC: (1 point)

Passwords and authentication

BASIC: (1 point)

Malware

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

Email ads

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

EXPERT: (5 points)

Spam

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

EXPERT: (5 points)

Prevention and mitigation

BASIC: (1 point)

INTERMEDIATE: (2 points)

Conclusion

1. Software-as-a-Service (SaaS)

Introduction

So, what exactly is SaaS?

Types of SaaS

Social SaaS

Shopping SaaS

Financial SaaS

Other SaaS

Privacy and security concerns

ToS and privacy policy

Service reliability

Security and transparency

Security breaches and response

Security updates

Data access

RohitRecommends

Types of SaaS

BASIC (1 point)

INTERMEDIATE: (2 points)

ADVANCED (3 points)

EXPERT (5 points)

SaaS privacy concerns

ToS and privacy policy (BASIC, 1 point)

Service reliability (ADVANCED, 3 points)

Security and transparency (EXPERT, 5 points)

Security breaches and response (INTERMEDIATE, 2 points)

Security updates (EXPERT, 5 points)

Data access (ADVANCED, 3 points)

Conclusion

1. Networks: Connectivity and Internet

Introduction

Wired networks

Wireless networks

Wi-Fi/WLANs

GSM

Bluetooth

NFC

Common attack vectors

Identification

Interception

Wireless attack vectors

Bluetooth

NFC

RohitRecommends

BASIC: (1 point)

INTERMEDIATE: (2 points.)

ADVANCED: (3 points.)

EXPERT: (5 points)

Conclusion

1. Operational Security (OPSEC)

Introduction

An adversarial approach

The OPSEC process

Dos and Dont’s

Mobile phone subscription

Device security

New signups

Conclusion

1. Epilogue

Introduction

Updated analysis

Conclusion

1. Bonus Chapter: Useful Tips and Tricks

The 10 Android permissions listed under “dangerous” protection level.

How to setup your Android without Google Services

Useful apps that you should definitely consider installing

Alternative app stores

For Android

For Apple

Conclusion

Checking your email on an unknown computer

Section 1

Introduction

Chapter 1

Prologue

Introduction

Hello, there! Before you dive into the rest of this book, I’d like to ask you to do something.

Take your smartphone, open the scanner app (or the camera app, if it supports QR code scanning) and scan the QR code that is printed on this page.

Open the link that is presented to you on your screen and follow the instructions on the page.

Alternatively, open the browser app on your phone and visit the following webpage:

https://leaktest.privacy.clinic

Now, you must have received a short alphanumeric code from the website. Note it down here:

This alphanumeric code will come in handy in future chapters. Note it here before you forget it!

When you are done, turn the page, and start your journey!

Before we begin…

We -- as in, you and me -- are going to make a few assumptions about what it means to ensure the security and privacy of your data by enumerating the following rules of data-sharing:

If the data is not encrypted and not in your control, then it is neither secure nor private. Storing your data unencrypted on remote servers is like keeping your data in an open book. Finding ways to access this data is the very definition of what hackers do day in and day out. For example, most of the leaks catalogued by services like HIBP (Have I Been Pwned), dehashed, and more.

If the data is in your control, but you can't encrypt it, then it might be private but it is not secure. A person with physical (or even digital) access to your data can still access it without your knowledge or permission. For example, plain-text passwords stored in browsers, or worse, in an Excel file on someone's PC!

If the data is encrypted, but not in your control, then it might be secure but it is not private. No matter how well it is encrypted, assume that an adversary already has access to it or might eventually have access to it. The toughest encryptions can (and will) be eventually broken, leaving you exposed to all kinds of potential attacks. For example, data stored on remote servers.

Only when your data is encrypted and in your control is when we can assume that your data is completely secure and private.

Two things to note:

You can never achieve 100% security and privacy of your data. The field of information security and privacy is always changing, with new vulnerabilities being discovered and new exploits being revealed every single day.

You can achieve close to 100% security and privacy of your data if you really want. However, this will require a LOT of technical know-how and expertise. You will also have to make many, MANY sacrifices along the way.

Don't get me wrong, I am NOT saying that security and privacy on the internet is an impossible goal! On the contrary, I'm saying that you do not have to trade ALL of your comfort for the privacy and security of your data!

The comfortability of data-sharing is a broad spectrum. It ranges all the way from people who are comfortable sharing all kinds of data with any third parties, to people who are uncomfortable sharing any kinds of data with all third parties. You can trade none of it or trade it all away, if you want – the choice is entirely up to you!

Who should read this book?

Everyone. Regardless of whether you are simply curious about privacy as a concept or have just begun your journey into securing your digital footprint, or you are a veteran of masking your presence online, this book will help you achieve the level of digital invisibility that you'll feel comfortable with.

I've attempted to keep this book as conversational as possible. While subsequent chapters will enumerate the potential risks associated with various devices, services, and many more, I will also enumerate ways to remove, reduce, or mitigate these risks.

Our endeavor throughout this book has been to provide insight into how your data is being shared with third parties—often without your consent—and what you can do to mitigate or, failing that, obfuscate it.

How to read this book?

I've tried creating this book as an interactive piece to work with. That means, at times, I will provide a QR code alongside the content. The QR code is meant for you to scan and read, watch, or do something on the internet and then return to the book. Think of these as the book-equivalent of hyperlinks that are meant to guide you to additional resources on the topic.

This book is meant to be a textbook and a workbook both—I highly recommend keeping your devices nearby while reading this book. As you progress through this book, you may identify some scenarios are directly applicable to you, while others may be irrelevant.

I will be providing you with various recommendations pertinent to the subject matter that is being discussed. Consider each recommendation carefully and choose whichever recommendation suits you best, that is, perform the tasks as instructed, immediately, on your phone, tablet, laptop, or online. Not every recommendation might apply to your specific scenario but some (or maybe, most) things will definitely apply. Choosing NOT to act on them would be a very bad idea.

I've also included a scoring system in the book to help you monitor your progress, as you read. This scoring system is based on the expertise and effort required to follow the aforementioned recommendations. You'll find these recommendations neatly tucked under a separate heading called #RohitRecommends.

What is #Rohit Recommends?

At the end of each chapter, I have presented several recommendations categorized neatly into four categories: Basic, Intermediate, Advanced, and Expert.

The recommendations under each of these levels are (mostly) progressive, that is, you'll (probably) have to fulfill the recommendations under the Basic level, before following the Intermediate recommendations. Each recommendation level is assigned a score, based on the amount of effort required to perform the tasks mentioned in the recommendation. In some cases, you might find only a single level of recommendation—that's probably because there isn't much else to recommend in that context!

Basic

Who: This level is intended for people who are curious about the privacy and/or security of their data and would like to have a clearer picture of how sharing (or not sharing) of this data might affect their digital experiences.

What: At this level, we will primarily gather information that will help you understand the security and/or privacy issues associated with the subject under consideration. In some cases, I may even recommend a few simple actions that you can take (almost) immediately, without significantly hindering your usage habits or your overall digital experience.

Example: If you are a heavy Facebook user who needs to continue using Facebook, I would recommend opening your Facebook settings and clicking on each option in the side bar, one-by-one, and turning off all the options that result in oversharing of your data.

Intermediate

Who: This level is meant for people who are concerned about their data being shared without their active consent and want to take steps to

mitigate it—provided it doesn't interfere with their daily experiences with digital devices.

What: At this level, we will utilize the information gained in the Basic level AND provide you with options that will help stem the leakage of your personal data. At times, I might even recommend tweaking a few system settings, a little bit. A rudimentary knowledge of computers and a superficial understanding of how the internet works would be considered an added bonus at this level.

Example: To continue the previous example, I'd recommend using a third-party app to access the Facebook service—preferably one that is more privacy-aware than the default app such as Simple Pro or Phoenix. We'd also recommend installing an ad-blocker on your device (that is, smartphone or computer) to further reduce giving away your details to unsecured third parties.

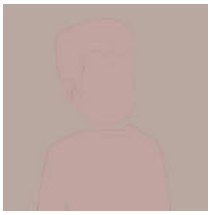
Advanced

Who: This level is meant for people who guard their privacy fiercely and would like greater control over their data. It requires a broader understanding about computers, (maybe) some bit of programming, and a more-than-superficial understanding of how the internet works.

What: At this level, we might require you to put your security and privacy concerns before everything else. A willingness to change long-standing habits and the ability to adapt to new situations and experiences will be very useful at this level.

Example: To continue the Facebook example, we recommend deleting the native Facebook app altogether and recommend that you use a privacy-aware browser—both on the desktop or mobile—for all of your Facebooking needs.

Expert



Who: This level is aimed at a very specific subset of people in society – people for whom maintaining privacy is a necessity, rather than a curiosity. Celebrities, law enforcement officers, soldiers, people enlisted in sensitive jobs such as the defense sector (that is, the army, navy, air-force, and many more) or people working in various intelligence services might want to consider this level.

What: At this level, you are expected to have significant knowledge of the subject matter under consideration and deep knowledge of the alternatives. I strongly recommend acquiring the services of a trusted person who can assist you with the same. A deep knowledge of computer systems, software programming (primarily working with APIs, web applications, and such), and a very good understanding of how the internet works is highly recommended.

Example: To continue the running example, we'd recommend that you stop using Facebook in its entirety. Instead, we would suggest that you utilize alternative methods of communication to reach out to your Facebook audience.

I strongly recommend that you consult with an expert (or experts) before attempting any of the Expert recommendations presented anywhere in this book. I shall not be held liable for any loss of any kind if anything goes against expectations or yields a less than desirable outcome, for those who insist on following any Expert recommendations without proper supervision or consultation.

Info

Advanced vs. Expert –What should YOU choose?

Many people recommend deleting your Facebook account entirely to ensure that Facebook cannot collect any data on you. However, this is somewhat misleading and, in some cases, against common sense.

For example, as a cyber-security expert, I need to use Facebook for two primary reasons: to promote myself and the various services I offer and for personal purposes.

However, I have taken great care to ensure that those two parts of my life (that is, personal and professional) are kept strictly separate on Facebook. There are various steps one can take to achieve a proper balance between being connected and staying private on Facebook. We'll be discussing all of these steps (and a lot more) throughout this book.

The points system

You already know about the four recommendation levels viz. Basic, Intermediate, Advanced, and Expert . You can choose to follow the recommendation that makes the most sense to you, and it doesn't have to be the same level in every case.

For instance, you can choose to follow the Advanced recommendations in the Chapter 9: Browsers , but only the Basic recommendation in the Chapter 10: Email .

Each recommendation is assigned a specific point score. In most cases across the book, a Basic recommendation is worth one point, Intermediate is worth two points, Advanced is worth three points, and Expert is worth five points.

Remember, you do not have to follow ALL the recommendations, only ONE of them!

Note

In some cases, you might find that the recommendations are progressive, that is, the previous level must usually be completed before proceeding to the next one. However, you DON'T have to follow them ALL the way. If you feel that the ADVANCED level is too technical or prohibitive, you may stop at the INTERMEDIATE level itself. You will then earn points for BASIC and INTERMEDIATE both, but not for ADVANCED or EXPERT.

You can keep a scoresheet of sorts by entering the points you 'earn' in any of the following places:

The Table of Contents

The Scoresheet at the END of the book

Print out of the softcopy of scorecard available on the website

After you finish reading/working through the book, tally up your points and see your progress. This will help you to get re-motivated to take more steps forward to further protect the privacy of your personal data.

Additionally, this book is designed in such a way that the information being shared by your phone/device changes with each recommendation you follow in the course of reading this book. You can track it for yourself, if you want.

Scan the QR code given alongside this paragraph or open the following link in your browser:

https://book1.privacy.clinic/scorecard

You'll need to enter the alphanumeric code (the one that you hopefully did note down at the beginning of the chapter) to access your privacy leak-test score. If you didn't note it down, don't worry – just go back to beginning of the chapter, scan the QR code, visit the webpage again, and generate a fresh code; and, this time, don't forget to note it down in the empty box provided on the first page!

Conclusion

A lot of people around me keep asking me what they can do to protect their privacy on the internet. Let me just put it this way. If there were a simple answer to this question, I would have simply tweeted it out instead of writing a whole book about it!

Don't worry though, it isn't as difficult as some of the articles want you to believe. Some of it involves some intricate steps but nothing that you can't do by yourself. In fact, that's the whole purpose of this book—to get you to question everything and take nothing at face value.

The ONLY thing I ask of you is this: Don't just read this book. Work with it, with me.

I've even tried to gamify this book by assigning points to various actions so that there is sufficient incentive for you to follow my recommendations.

You may not like the points system, but believe me when I say that it works like a charm. Keep telling yourself that your target for this book is to score as many points as possible in the next 12 chapters. You don't have to score the maximum every time. Just like a cricket match, score singles and twos here-n-there and hit the occasional full-toss over the ropes!

If you do, I can assure you that it will help you gain control over your data, your privacy, which is supposed to be YOUR choice.

Chapter 2

Internet and Privacy

Introduction

Imagine you were rich – like, pre-divorce Jeff Bezos' kinda rich.

Imagine that you decided to hire a personal assistant, like a butler. Except, this butler would take care of everything for you, up to the point where all that remains to do is making a yes-or-no decision. What's more, your butler also notes down your preferences and updates their suggestions accordingly the next time. Your morning would end up looking something like this:

Your butler comes in to wake you up at 6 AM. You could wake up ("Yes.") or you could refuse to wake up ("No…").

Butler's Notes: "0600: Did not wake up."

He comes back five/ten/fifteen minutes later and repeats the question until you decide it is time to wake up.

Butler's Notes: "0605: Did not wake up"

Butler's Notes: "0610: Did not wake up but seems partly awake."

Butler's Notes: "0612: Woke up. Number of wake-ups required: TWO. Time between first wake-up call and actual wake-up: 12 minutes"

He then offers you the morning newspaper along with tea and breakfast in bed. You could accept it ("Yes.") or refuse it ("No…").

Butler's Notes: "0615: Accepted tea. Refused breakfast-in-bed."

Then you go shower and start getting ready for the day.

Butler's Notes: "0629: Went to shower."

Your butler now presents you with your clothes. You reject his first suggestion of a black shirt ("NO."), reject his second suggestion of a purple shirt ("No…"), and accept his suggestion of a pink shirt ("Yes.").

Butler's Notes: "0645: Came out of shower. TOTAL SHOWER TIME: 16 minutes"

Butler's Notes: "0646: Rejected BLACK shirt."

Butler's Notes: "0647: Tried PURPLE shirt. Rejected."

Butler's Notes: "0648: Chose PINK shirt. TIME TO CHOOSE: 2 minutes"

You get the general idea, right?

Over time, your butler builds up a pretty accurate idea of your choices and preferences. He is able to make suggestions that are so perfect that you simply can't refuse! It's like he knows you inside and out! He is the Jeeves to your Bertie Wooster, and you absolutely couldn't live without him. In fact, you have come to trust him so blindly that you don't bother reviewing your options and just end up accepting the first option he presents to you. Hey, it saves you time and your butler just seems to know what you like, doesn't he?

Except this butler isn't Jeeves and lacks one crucial quality – loyalty.

While you were blindly trusting him with some of the most intimate details of your life, your butler was selling those notes he was making about you to the highest bidder. You've heard whispers of it happening but it doesn't bother you. After all, what difference does it make if he tells people what color shirt you prefer to wear, right?

Turns out that the information collected by your butler was used by your grocer to sell you a more expensive tea. It was used by your designer to dress you up in darker shades. It was used by your newspaper agent to sell you a subscription to a brand of journalism that espouses slightly more left-leaning (or right-leaning, depending on your preference) point of view.

So, although you didn't notice it at first, things have certainly changed since he took over your life. Your brand of tea is different, you wear darker shirts more often, and you no longer read The Expressive Indian; you now read the The Times of Timbuktu instead!

By now, you must have latched on to the fact that this hypothetical example isn't entirely hypothetical.

The butler in question could be your smartphone. Or your smart TV or your smart refrigerator or your fitness tracker. Any internet-connected device, really.

Because that's exactly what they are meant to do. Gather data, and build your profile. A profile that can be used by various advertising networks to show you ads on the various sites you visit on the internet, like Google, Facebook, Twitter, Instagram, to name a few.

Privacy? What privacy?!

A 2018 report published jointly by IAMAI and Kantar-IMRB estimated the number of mobile internet users to be around 500 million. Judging by the growth pattern in recent years, we could say that the number of mobile internet users is rapidly approaching a 1:1 ratio, that is, every adult carries a device capable of connecting to the mobile internet.

Did you know, the technology that exists today allows each one of those 500 million users to be uniquely identified?

Google

When you sign into a Google account on your smartphone, Google generates a unique identifier for your phone called the Google Advertising ID. You can verify this yourself. If you have an Android phone, open your Settings | Google , then under Services , click on Ads . You'll see the advertising ID assigned to you by Google at the bottom; it'll look something like this:

Your advertising ID:

x12xxxx3-456x-7xx8-xx90-xx1xx2345x6x

Hint

You can opt-out of Google’s Ad personalization by toggling the switch that you see here, that is, you’ll still be shown Google’s text ads on various sites but Google will not associate your browsing behavior and your usage across various Google accounts to personalize these ads in any way.

Everything you do on your Android phone is being relayed to Google's servers, and their algorithms are crunching all the data to figure out what your likes and dislikes are and how best to serve you content and ads that are tailored to your likes and dislikes.

It’s not just Google, by the way.

Microsoft

In the summer of 2015, Microsoft released Windows 10 and offered it as a free upgrade to all Windows 7 users – genuine and otherwise. Many users took them up on the offer without realizing that Windows 10 sends a lot of telemetry information back to Microsoft servers by default. Even if you choose the option to NOT share any information, Microsoft collects what it calls Basic diagnostic information.

Have you ever wondered what is included in Basic diagnostic information? Well, Microsoft has been kind enough to tell us themselves!

"Basic: Send only info about your device, its settings, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up-to-date, troubleshoot problems, and make product improvements."

You can see this for yourself by opening Settings | Privacy and clicking on Diagnostics & Feedback in the sidebar.

Facebook

When you grant an app on Facebook the permission to read your profile, Facebook shares your unique Facebook ID; your first, middle, and last name; your picture; your email; and a list of the pages you manage freely with the app. In most cases, developers of apps will include broader permission requests as well, and ask you for your birthdate, your friends list, and your gender.

…and this is just the data that can be extracted WITHOUT human intervention!

Cambridge Analytica

If you are wondering why you should be worried about a bot that broadly sweeps available information, I have two words for you: Cambridge Analytica.

An academic researcher called Aleksandr Kogan developed a Facebook personality quiz app called This is Your Digital Life , which was used by a

company called Cambridge Analytica to gather information on about 80 million Americans in 2014.

The exact data-points that were available to the app are not precisely known, but, based on freely available information on Facebook's Graph API, we can safely estimate that they definitely had access to (and almost certainly acquired information pertaining to) all of the following data-points for all users who took the personality quiz:

Table 2.1: A (non-exhaustive) list of the various data-points accessible to Cambridge Analytica through Facebook's Graph API.

What made the whole thing worse was that the way Facebook permissions were designed, the app could access not just your information but also the information of all the people in your friends' list. So, even though only handful (estimated to be about fifteen hundred) users took the quiz, they (allegedly) ended up leaking details of around 80 million others.

Moral of the story? The next time you are invited to figure out which Marvel character you are, remember Cambridge Analytica, will you?

Info

"The Great Hack" on Netflix.

This 2019 documentary follows the Cambridge Analytica controversy in great detail—beginning with the shady methods used by CA to acquire profile data of users, right up to the investigations carried out by lawmakers in the US Congress and in the UK Parliament.

Cambridge Analytica collected about five thousand data-points to build accurate psych profiles for millions of Americans. They then were hired by various political clients (for example, Barack Obama, Ted Cruz, Donald Trump, Brexit, and many more) to promote stories on their Facebook timelines that subliminally encouraged them to vote in a certain manner.

To do this, they did not need to convince all of the voters in a specific geographical zone; they simply chose to convince only the number of people who were on the fence and swing their beliefs in the direction they wanted. Such people were called persuadables and the documentary goes into some amount of detail about how they were identified and categorized by an automated algorithm. I recommend you definitely watch it, whenever you get a chance.

All of your devices that are connected to the internet are constantly relaying various bits of identifiable information about you—information that can be merged and consolidated to create a larger picture of you and/or your life.

Of course, you could argue that these devices and services are trying to make your life easy by keeping a detailed track of your likes and dislikes. If that's what you believe, well, more power to you.

However, there might be some among you who are concerned about the amount of information being collected about you and your activities. There might be some among you who would like some semblance of control over the information (and the huge amounts of it) that is being shared with various entities.

If you are one of these people I just described, then this book is exactly what you need.

Adversaries and threats

All this while we've been discussing bots and programs (such as the one used by Cambridge Analytica, for instance) that are designed to automatically sweep information about you by casting a broad net.

Let's raise the stakes a little bit. What if someone *specifically* wanted to find out information about YOU? Could they get their hands on it? What kind of information could they get their hands on? Something public? Something private? Would they be able to take advantage of this information?

The simple truth is this: Wherever there is private and/or personal data that requires protection, there will always be some kind of an adversary looking to acquire it in some unauthorized manner. With the introduction of internet-capable smartphones, the number of people accessing the internet has increased, and so has the number of malicious actors. Nigerian Prince scams are outdated; modern scammers can now employ much more sophisticated tools and techniques to con people.

In other words, adversaries on the internet have gotten a lot smarter. You need to be a lot more aware of them now than you were in the past. You need stay eternally vigilant and keep learning how to proactively defend yourself from any adversarial attacks on your private and/or personal data.

To do that, you need to understand who your adversaries are. So, let's quickly look at a few common types of adversaries and/or threats that you might encounter on the internet.

Passive adversaries

A passive adversary is someone who is not targeting you or your credentials but will gladly use your credentials to further act upon whatever malicious intent they may have.

Most 'hackers' on the internet can be classified as passive adversaries, since they look to acquire vast compilations of private and/or personal data without actively meaning to target any specific person. Also, since passive adversaries do not target you specifically, there is rarely any indication of your data being compromised until it gets used by an active adversary.

Note

There is a distinct possibility that your current email credentials, banking credentials, contact details, home address, etc. have already been accessed and sold by/to a passive adversary.

Active adversaries

An active adversary is someone who is specifically trying to gain access to YOUR private details.

Active adversaries make specific efforts to acquire any data that you may deem personal and/or private, such as your email credentials, your banking credentials, your home address, your contact details, and more. It is relatively easier to identify attacks by active adversaries than attacks by passive adversaries.

A passive adversary may (or may not) become an active adversary depending on whether (or not) they become specifically interested in you. Conversely, active adversaries may employ hacking techniques commonly employed by passive adversaries to get to your personal/private data.

Intrusive advertising

While intrusive advertising is considered by many as harmless, the Cambridge Analytica episode is proof enough that the data collected by advertisers can be weaponized to create psych profiles of individual users. A well-built psych profile can be used to manipulate users by feeding them information specifically designed to either alter or enhance their beliefs and perceptions.

Furthermore, intrusive advertising can also create false associations through incorrect marriage of collected data. A person searching for a tyre and a rope may not necessarily be looking to build a swing in their backyard, you know?

Invisible threats

Adversaries that are able to remain hidden before, during, or after an attack on your digital existence are what we classify as invisible threats.

This doesn't mean that such adversaries cannot be seen; it means that they may be so adept at covering their tracks that they are able to leave little to no trace of ever having existed. Hollywood uses the popular phrase 'ghost in the shell' to describe such invisible adversaries. Such adversarial techniques require significant knowledge and resources in order to ensure near-perfect execution. Typically, such knowledge and resources are usually available with either state actors or a handful of highly intelligent and dedicated cybersecurity professionals.

Note

While these categories broadly cover any potential adversaries you may encounter, this list is in no way neither exclusive nor exhaustive. More categories of adversaries may (or will) be discovered as we discover new ways of interacting in the digital world.

What we already know about you

I have a confession to make.

Remember, in the first chapter I asked you to scan a QR code and open a webpage. Well, I wasn't being entirely honest with you there.

When you opened that webpage, you sent me a ton of data about you, your internet-connected device, your network, and a whole host of details about you that you probably didn't even know existed.

Don't worry, I am not going to use this data for any nefarious purposes – you have my word. In fact, if you want to see what data I was able to

collect from you, simply scan the QR code shown alongside this paragraph and enter the alphanumeric code that you noted down (in the empty box) in the first chapter, earlier.

Alternatively, open your browser app and go to the following webpage:

https://leakscore.privacy.clinic

I just wanted to show you how much of your personal information is sent out there without you even knowing/realizing that you just gave it out. If you followed the instructions correctly (and if I was right in my assumptions), then I was probably able to correctly identify at least a few of the following:

Your mobile device make and model

The location where the picture was clicked (maybe)

Your preferred browser

Your location

Your telecom/internet service provider

Your physical location (maybe)

…and a few other things.

How would any of this help me, you wonder?

Well, some (or all) of this data, combined with your first and last name, would allow me to track down your social media profiles, which could possibly yield your birthdate. Using that, I could try and reset your email password, assuming you don't use any kind of Multifactor Authentication (2FA) on your email account.

If I am successful in gaining access to your email inbox, it could provide me with a plethora of valuable information, such as your bank account details, your secondary email address, not to mention your most frequently emailed contacts—in other words, names and email addresses of your loved ones.

Furthermore, if you are the kind of person who reuses the same email address for logging in to various sites, I could also try resetting the password to your bank accounts, and I get the feeling that I would probably be successful there as well.

…but you don't have to worry, I am not going to do anything of the sort. Scout's honor. I just wanted to give you a taste of how bad things could get, if you continued to remain careless.

In fact, how about you try it out yourself?

Come; let me guide you through the basics of snooping on yourself, using just simple search terms on Google.

The basics of snooping

Let's start with a simple search on Google.

Say, you are one of those people who have a rather common name, for example, Amit Sharma or Rajesh Patel . The search results page is obviously going to throw up a lot of results. That is, however, not a problem. Simply add site: facebook.com to your search terms, that is, instead of searching for Amit Sharma , we'll now search for Amit Sharma site:facebook.com.

Note

I'm deliberately choosing the name Amit Sharma here because Amit is one of the most common Indian names and Sharma is also a very common Indian surname. To any Amit Sharma's that may be reading this, my apologies, I didn't mean to target you specifically!

What we're telling Google here is something along the lines of; Show me only the results for Amit Sharma which has come from facebook.com. Typically, the first result from Google will be a link titled Amit Sharma Profiles with a link such as:

https://www.facebook.com/public/Amit-Sharma

Okay, this tells us that there a LOT of Amit Sharma's in the world! It will take us ages to scroll through all of them and identify them by their photos! Let's see if we can narrow the results by tweaking our search terms a little bit. Let's add in the city where you live to the search term, that is, let's search for Amit Sharma Pune site:facebook.com.

Most of the time, these two steps are enough to identify a relevant Facebook profile—in this case, YOUR Facebook profile. Open this profile in an incognito/private window to see what information is being made publicly available by facebook.com to the world.

For instance, in the case of Amit Sharma from Pune, you'll notice straightaway that Facebook immediately tells you where the person works, where they have studied, what their 'likes' are, etc. It even helpfully lists other people with the same name in case this is not the profile you are looking for.

…and that's just in the incognito window!

Someone who is logged into Facebook and on your friend list will, obviously, be able to acquire a lot more information by accessing the various tabs on your Facebook profile, that is, About, Friends, Photos, and (ironically) more. In some cases, I have been able to find birthdates, addresses, and even mobile numbers and email addresses on the About tab itself!

Advanced snooping or OSINT

OSINT , short for Open Source Intelligence , refers to the practice of uncovering valuable information about a particular target using openly available data.

This image posted on a blog post titled, The Ultimate List of 50 Free Security Tools, Tested For You on the Heimdall Security Blog, gives a good idea of how a complete picture can be derived by systematically searching/accessing information from various online sources:

Figure 2.1: Various online sources for sourcing OSINT information (Source: https://heimdalsecurity.com/blog/free-cyber-security-tools-list/)

Note that some of the sources mentioned in the image may not qualify as freely available, but the image still manages to provide a good idea of how OSINT works.

Coming back to our example, using only a name, city of residence, and the knowledge of what someone looks like, (in this case, that someone being you), I was able to help you track down your Facebook profile. The profile page would further yield crucial information, such as workplace, education details, and a bunch of other information that can be further used to identify relevant profiles on other social networks in future searches.

…and we haven't even opened Twitter, Instagram, or any of the other social networks yet!

Acquiring your address isn't very difficult either…

Imagine receiving the following call:

"Hello, is this Amit Sharma? Congratulations! You have won a toaster in our lucky draw! Which lucky draw? Well, every month, we reward a few lucky customers who purchase from Flipkart! Could you please confirm your date of birth and your postal address to ensure that we have got the right Amit Sharma? It is such a common name, you know?!"

…or alternatively, getting this SMS:

"Congratulations, Amit Sharma! You have won a toaster from Flipkart! To get your prize delivered, please WhatsApp a copy of your ID and address proof to +91 98XXXX XXXXX within 24 hours of receiving this SMS."

Sure, you may be smart enough not to fall for this scam, but these examples were just a way to illustrate how easy it is to acquire your home address through a simple phone call or SMS. A smart adversary will probably even carefully customize the pitch in a manner that will sound completely believable.

Conclusion

I want to clarify something here: My intention in this chapter is not to alarm you.

That said, if this chapter alarmed you, good. As wonderful as the internet is, it is also a place where we unknowingly give away tons of information about us. The examples I outlined in this chapter have convinced you just how easy it is. If you still don't believe me, think of the first person you met today. Now, use the techniques I followed in this chapter and see how quickly you can figure out the following details:

Their full name

Their date of birth

Their postal address

Their email address

Their mobile number

So, how long did it take you? Not very long, I presume?

Here's the thing, if this little example above has served as a wake-up call of sorts for you, then this book is exactly what you need. Sit down with your smartphone, or your PC, or your smart device, and make the changes that I recommend at various points in this book. Make the effort to secure your data.

I am not going to promise that this book is a silver bullet for all your security needs.

Security and privacy isn't a solution that you can implement—it is a lifestyle that you must adopt. I am here to teach you a lifestyle, if you are willing to put in the effort to learn it.

Are you ready?

Section 2

Devices

Chapter 3

Android Devices

Introduction

All smartphones -- be it an Android, an iPhone, or a Windows [1] phone -- leak data.

If you are using an Android-based (or Android-equipped) phone, your phone might be sending tons of data back to Google -- often, without your knowledge and/or consent. If you're using an iPhone, it is probably sending data back to Apple -- although not as much as Google, I believe.

To be fair, the entire Google ecosystem is designed to aggressively collect data about your interests and show you ads that are most relevant to your interests. In contrast, Apple labels itself a product company and has strongly distanced itself from any and all privacy-intrusive data collection.

So, which of them is the better option?

Over the next few chapters, we'll be enumerating the various privacy issues in smartphones and how to deal with them. We'll begin with the Android OS and then look at iOS separately [2] , and finally look at the apps on your smartphone that might be sharing crucial information without your knowledge and/or consent.

The Google-Android ecosystem

We know that the Android OS is developed and maintained by Google. However, that should not be taken to mean that Android is Google or vice-versa. Android is just a product developed by Google, and it uses a lot of Google's services. However, these services are not necessarily required or mandatory for running Android on a compatible smartphone.

Confused? Well, let me explain…

While Google does have a significant presence on Android-equipped and Android-enabled smartphones, it does not mean that Google develops everything in the entire Android ecosystem. In fact, many phone manufacturers prefer to adapt the Android OS to their own brand and create something different.

To understand this somewhat complicated relationship, imagine AOSP as the engine of a racing car. Google also, incidentally, happens to be the manufacturer that produces other essential car parts such as the steering, transmission, wheel, tires, internal wiring mechanism, and more.

Each racing team (that is, phone manufacturer) has the freedom to build their own chassis (that is, handset models) and slap their own livery (that is, user interface) on it to manufacture their own custom version of an Android-based machine -- think Red Bull using Ferrari engines or McLaren using Mercedes engines in F1 races.

At the heart of it, these phones still run on Android and the internal mechanisms are still provided by Google, but each racing team is free to make additions as they please. Some merely change the livery (for example, Samsung and HTC) while others make changes to the internal wiring (for example, OnePlus and Xiaomi) before selling the machine to customers.

In case you were keeping track, this makes the Google Pixel [3] phones the (closest) equivalent of a stockcar since it runs the AOSP engine (which is developed by Google) and all essential parts and livery are designed by the same manufacturer that manufactures the engine , viz. Google.

For example, the TouchWiz UI on most Samsung phones is mostly an enhancement of the stock Android UI, but Samsung also includes a few exclusive third-party Android apps with its phones. Other phone manufacturers may choose to make far more comprehensive changes, for example, MIUI OS on Xiaomi phones. Not only is the MIUI OS designed to (somewhat) emulate the iPhone user interface; it also collects a staggering amount of data. This data is then processed to show us relevant advertisements in the form of Suggestions and Recommendations *within* the OS itself!

This analogy holds up well with upgrades too.

Like all engine models undergo improvements from time to time, so does AOSP. If you wish you can choose only to buy the latest model (that is, buy the new Google Pixel). The teams can choose to upgrade just the engine, or make cosmetic changes, or design a completely new chassis, or maybe even do everything at once.

All of this is singularly possible, thanks to the Android Open-Source Project(AOSP).

Android Open-Source Project (AOSP)

Here's how the official Source website describes the Android Open Source Project or AOSP:

Android is an open-source software stack created for a wide array of devices with different form factors. Android's primary purpose is to create an open software platform available for carriers, OEMs, and developers to make their innovative ideas a reality and to introduce a successful, real-world product that improves the mobile experience for users.

— (https://source.android.com/setup/ , as on July 20, 2019)

Simply speaking, AOSP isn't a complete OS by itself; it is merely the platform on which the rest of the Android OS is built. Anyone can use this platform and build something else entirely on top of it, while still calling it Android.

Remember what I said earlier?

AOSP is the engine and the various applications and services provided by Google are the essential components (steering, transmission, wheels, tires, internal wiring, and more.) that make up the basic skeleton of the car.

These applications and services that Google provides actually have a name – they are called Google Mobile Services (GMS). According to the Android – Google Mobile Services page: (https://www.android.com/gms/)

While the Android Open Source Project (AOSP) provides common, device-level functionalities such as email and calling, GMS is not part of AOSP. GMS is only available through a license with Google and delivers a holistic set of popular apps and cloud-based services.

So, why does Google do this?

To put it simply, AOSP is Google's way of maintaining a viable alternative to its biggest competitor in the market – Apple's iOS. By making the

AOSP free to use, Google ensured two things:

Cheaper smartphones: Every smartphone manufacturer – past and present – had an inexpensive (read: free) option for an - operating system to put on their smartphone hardware. This meant that companies could make and sell Android-enabled or Android-equipped smartphones for far cheaper than Apple iPhones.

More Google/Android users: The more the people buying Android-enabled or Android-equipped phones and devices, the more the traffic for Google and its products and services.

You see, Google develops and maintains the Android source code, that is, keeps it clean and tidy, keeps it up-to-date, and makes it available for people/organizations who might want to use it.

Of course, Google does all of this under a very liberal license that allows different people to utilize the code differently, according to their needs. That means, Samsung can tweak the code to bundle in their TouchWiz UI and Xiaomi can tweak it to give their users, their heavily modified version, that is, MIUI.

However, it also means that Google gets to decide the direction the AOSP takes. They get to decide what features are to be developed and incorporated into AOSP and by extension the stock Android OS. It also means that Google can tweak AOSP to include the code necessary to collect whatever data they wish from people who just happen to be using some version of the Android OS – stock or otherwise.

What is a ROM?

In the world of Android, ROM refers to the read-only part of internal storage, which contains the operating system.

The read-only attribute of the internal storage ensures that no changes that can cause the device to malfunction can be made. These official ROMs are also called firmware sometimes since the software stays firmly in place, that is, regular device users are not allowed to make any modifications whatsoever.

Info

Why are they called ROMs?

The term 'ROM' comes from the era of CDs and DVDs -- technically called CD-ROMs and DVD-ROMs, respectively. The ROM in their names stood for Read-Only Memory, that is, the memory that cannot be erased or rewritten.

However, in case of Android, modification of firmware/official ROM is not impossible -- the only deterrent in most cases being a software or hardware lock. Hardware locks require specialized devices to unlock them, whereas software locks can be overridden by using special software written for the express purpose of performing this task.

Official ROMs

Official ROMs or firmware are usually of two varieties:

The Google Android OS commonly referred to as Stock Android

A customized Android commonly referred to as Firmware

Only a select few devices ship with the stock Android OS, such as the Google Pixel series, Nokia 6 and 8 series, the Xiaomi Mi A-series, and more. In most cases, manufacturer-branded firmware often has some enhancements added over the stock Android OS. These enhancements range from simple interface enhancements to severe usage restrictions.

Sometimes, firmware may be customized and branded either according to the manufacturer or the telecom service provider. In rare cases, your device may have firmware that has been customized by BOTH manufacturer and the telecom service provider, although this is mostly a US thing. Most Indian telecom service providers do not offer such locked devices -- customers are free (and often encouraged) to purchase their own devices.

In some extreme cases, the customizations to the stock Android OS maybe so substantial that an argument can be made about them being more of custom ROMs, rather than manufacturer-branded firmware.

Custom ROMs

Thanks to AOSP being open-source, many independent developers have attempted to customize the OS in very specific ways for their favorite devices by making modifications to the source code. These developers often tend to release their tweaked code for the general public to use as custom ROMs.

In simple words, a custom ROM is an 'unofficial' firmware for a specific phone made by some independent developer(s) that has been released to the general public.

Some popular custom ROMs that are available for a wide variety of devices are Lineage OS, OmniROM, Replicant OS, SlimROM, Paranoid Android, Resurrection Remix, and AOSP Extended.

Info

The very first piece of tech that Xiaomi (the phone manufacturers behind 'flagship-killers' such as the Redmi Note 5 and the Pocophone F1) released was actually a custom ROM for several popular Android phones called MIUI, back in August 2010. A year later, the Xiaomi Mi 1 smartphone was announced. The developers of CyanogenMod, another popular custom ROM, had a deal with OnePlus for a while. However, that deal ended after OnePlus decided to ship their phones with OxygenOS instead. CyanogenMod goes by a different name these days; you probably know it as LineageOS!

XDA, the go-to forum for all things Android, has a detailed post describing the most popular custom ROMs for Android phones, here:

https://www.xda-developers.com/the-most-popular-custom-roms-on-xda/

Scan the QR code given alongside this paragraph to read a quick overview of the most popular custom ROMs on the XDA forums.

Official firmware vs custom ROMs

Unlike stock firmware, custom ROMs can be notoriously unstable. However, custom ROMs are also developed and tested at a rapid pace, with some popular custom ROMs even pushing out updates on a nightly basis!

On the other hand, stock firmware goes through rigorous testing and scheduled release cycles. However, this also means that updates may take a long time to ultimately reach end-users -- especially if they live outside of the continental United States.

Given below is a table that shows the major differences between official firmware and custom ROMs. Note that this table covers most of the major differences but should, in no way, be considered exhaustive:

Table 3.1: A non-exhaustive comparison between official firmware and custom ROMs.

Based on this table, one might feel that rooting your phone and/or installing a custom ROM is the smartest thing you can do with your Android phone. However, before you do that, remember that installing a custom ROM might void the warranty on your phone. Think carefully and evaluate whether you really need to install that custom ROM on your Android phone before you decide to go through with this decision.

Android and privacy

Google constantly strives to make Android a secure OS. However, the open nature of the platform means that developers of various Android ROMs (both manufacturer firmware and custom ROMs) can attach additional programming to their ROMS to compromise the privacy of your personal data.

Most manufacturers claim that they are actually providing a service by allowing users to retain cloud-based backups of their data. However, that makes these backups immediately vulnerable to malicious actors, who might try several illegal methods (discussed in the previous chapter and throughout this book) to acquire this data.

This is not to say that people with Android-based or Android-equipped phones cannot hope for privacy. Like with all other things, it is difficult but not impossible.

In the following sections, I will outline some of the privacy concerns and then explain what you can (or rather, must) do to mitigate them and regain control over your personal data and how it is shared.

Google Telemetry

Let's make something perfectly clear: Google is in the business of collecting your data. If in the process, they have to give something away for free, they are very likely to do it and often without a second thought.

Google still makes most of its money by serving contextual ads on webpages, i.e. ads that are relevant to you AND the webpage you are viewing. That's why you might see ads for shoes on a webpage on your device, but your wife might see ads for jewellery on the same webpage on her device. To decide which ad to display for a particular user, Google collects information from its various 'free' products and offerings.

Thus, every time you open Gmail, search for directions on Google Maps, watch a video on YouTube, search on Google, view a webpage in Google Chrome, read documents in Google Doc, listen to a podcast episode in Google Podcasts, upload files and photos to your Google Drive, connect to your car entertainment system with Google Auto, cast your screen using a Chromecast, call someone using Google Duo, download an app on the Google Play Store, translate stuff using the Google Translate app, you are sharing a lot of information with Google.

Info

Did you know, in 2014, Google bought a smart thermostat-manufacturer called Nest for $3.2 billion in cash?

Nest (at the time) made smart thermostats and smoke detectors that could speak to each other and to other Nest devices across the internet. Google, at the time, was primarily in the business of displaying ads to users across the internet. So, the question that arose was obvious?

So, why was Google interested in the Nest? Was Google planning to broadcast ads on their tiny smart-screens?

Actually, the data these devices were gathering was just the beginning of the revolution we know today as IoT - the Internet of Things. Google had realized that by gathering information about how you used various appliances at home, they could create a more complete profile of you. In fact, in Feb 2019, Google confirmed in that Nest has a hidden microphone but it had erroneously omitted it from its tech specs.

If you are thinking that they were going to use this profile to serve you with more contextual ads, you would be absolutely right…

In fact, if you want to know what information Google stores about you, simply visit the following link:

https://takeout.google.com/settings/takeout

…and download your data. In fact, here's a handy QR code that you can scan, which will take you straight to the Google Takeout page.

Go ahead and scan it. Trust me; you'll be surprised at the length and breadth of information Google has about you.

Non-Google Telemetry

All manufacturers who customize AOSP for their respective devices indulge in attempts to collect user data from Android devices, even Google. In fact, the stock Android OS itself has a ton of telemetry options that relay various bits of information back to Google servers.

With non-Google manufacturers, devices may send a lot of telemetry data to servers, sometimes, outside the home country -- depending on where the device manufacturer chooses to install these servers. This data may or may not be scrubbed; that is, it may still contain elements that can be used to identify you, thereby rendering your privacy compromised personally.

OnePlus Telemetry

In 2017, a security researcher named Chris Moore found that OnePlus phones were sending sensitive user data back to Chinese servers without permission. Subsequent investigations revealed that users had found traces of similar behavior on their older OnePlus devices going as far back as 2016.

When the story broke, OnePlus apologized and made changes to how their devices collect data and made the whole thing an opt-in, by calling it the User Experience Program .

Xiaomi Telemetry anddata breach

It was suspected that Xiaomi phones were sending critical private information (such as the IMEI numbers, address books, and messages) to Chinese servers. These suspicions were revealed to be true in 2014 when an independent Taiwanese researcher found a critical security flaw in the Xiaomi website code that exposed a ton of user details. The researcher claimed that he could access the credentials of millions of Xiaomi accounts and logs from the servers.

Xiaomi investigated the claim and subsequently issued a statement denying both the vulnerability and the leak. They counter-claimed that the data being claimed by the Taiwanese researcher was from 2012 and not 2014 as was being claimed. It was also obsolete since they had switched to a different account system.

To their credit, however, Xiaomi immediately asked their users to reset their passwords and publicly announced the incident as a way to mitigate any potential fallout from this incident.

…and others!

Around the same time as the Xiaomi story broke, Sony Xperia phones were also found secretly transmitting user-data to Chinese servers using similar spyware. There have been several reports over the last few years of other well-known Android devices [4] phoning home as well.

Recommendations and suggestions

You may have noticed some variation of Recommended Apps or Suggested Apps being displayed on your non-Google Android phone. Some of these may be due to an adware-infected app, while others may be due to the firmware or the OS itself!

Xiaomi, for instance, has recently been found to be inserting advertisements in the OS itself. In its most recent OS update for its phones, that is, MIUI v10 recommended apps were spotted in at least eight different places in the OS. Xiaomi subsidizes the cost of the phone by providing these recommendations , which are usually paid for by creators of the app or service being advertised.

In other words, they are leasing out advertising space on your phone, and they are doing so without your permission.

Huawei, Honor, and a few other lesser-known phone manufacturers have also been caught pushing lock-screen ads on the devices of unsuspecting users in the past. Both Huawei and Honor have since made changes, and the ads are no longer visible on their devices.

Sensors

In addition to your GSM/CDMA and Wi-Fi radios, most modern phones these days are equipped with a variety of sensors such as GPS, Bluetooth, Near-Field Communications (NFC), accelerometer, etc. All of these sensors are designed to share data freely, and your phone is constantly communicating all kinds of data to the outside world, through these radios and sensors.

I even showed you a simple demonstration of this data-sharing in the first chapter, remember?

By simply making you visit a webpage, I was able to determine a bunch of things about you and your phones, such as your location, IP address, saved networks, and more.

Sure, there are legitimate instances where sharing this information is useful and/or necessary.

For instance, you might want to share your location with someone when you are planning to meet with them. Or you might want to orient yourself when you land in a new city. Or you might want to evaluate your network to see if there is any vulnerability.

However, each of these situations demands active participation and consent. Therefore, the simplest (and the best) course of action would be to switch on these sensors only when required and switch them off as soon as you are done. The details on how to achieve this are provided under the #RohitRecommends section at the end of this chapter.

Permissions

In most cases, apps on your Android device cannot automatically access any sensor data just because they are installed on your device -- they need to be given explicit permission. Apps will request this by presenting you with a small dialog box [5] that says, Allow [XYZ app] to access this device's location? when you open the app.

Not all permissions need to be explicitly granted, however. According to the documentation available on developer.android.com:

The purpose of permission is to protect the privacy of an Android user. Android apps must request permission to access sensitive user data (such as contacts and SMS), as well as certain system features (such as camera and internet). Depending on the feature, the system might grant the permission automatically or might prompt the user to approve the request.

This differentiation in permissions (called Protection Levels in the official Android documentation) was introduced from Android version 8.1 Oreo. There are three protection levels that affect third-party apps - normal, signature, and dangerous permissions:

Normal permissions are those that are required when the app needs to access data outside its own sandbox, but the data that it is trying to access doesn't risk the user's privacy, for example, permission to access the user's time-zone.

Signature permissions are those that are given to certain system-critical apps included on the device by the manufacturer and typically grant

access to certain system-level actions. At times, these apps cannot be uninstalled or disabled by the user.

Dangerous permissions are those that are likely to affect the user's privacy or the operation of other apps. The user is prompted to give permission to the app explicitly and the app cannot provide the underlying functionality until the user has explicitly approved the permission request.

For example, in the example above involving the GPS/location sensor and the XYZ app, if the user denies the GPS/location permission to the app, the app will not be able to display the user's current location on the screen.

I've detailed these permissions in the last chapter of this book, under a heading titled, " The 10 Android permissions listed under 'dangerous' protection-level", in case you are interested in knowing what these dangerous permissions are, and how they affect the privacy of your personal data.

RohitRecommends

Almost all of the current Android phone manufacturers have a significant vested interest in learning about your phone usage patterns. Getting to know how the average user uses their phone allows them to design the user experience in a way that enhances the utility of their phones for the user.

On the surface, this might seem benign, but the potential for misuse of this data is huge. At the very least, this dataset is ripe for targeted advertising. Therefore, it is in every user's interest to ensure that Google and other manufacturers get their hands on as little data as possible.

Google Telemetry

It is extremely important to be aware of what data you and your device may be shared with various entities. To get an idea about what your device is sharing with Google, you can check the My Activity section in your Google account.

Open the Google Settings app on your Android device. If you don't see a Google Settings app, open the Settings app and click the Google section to open it. Click on Google account at the top to open your account page. Open the Data & Personalization tab and click the link titled, Manage your activity controls at the bottom of the Activity Controls section:

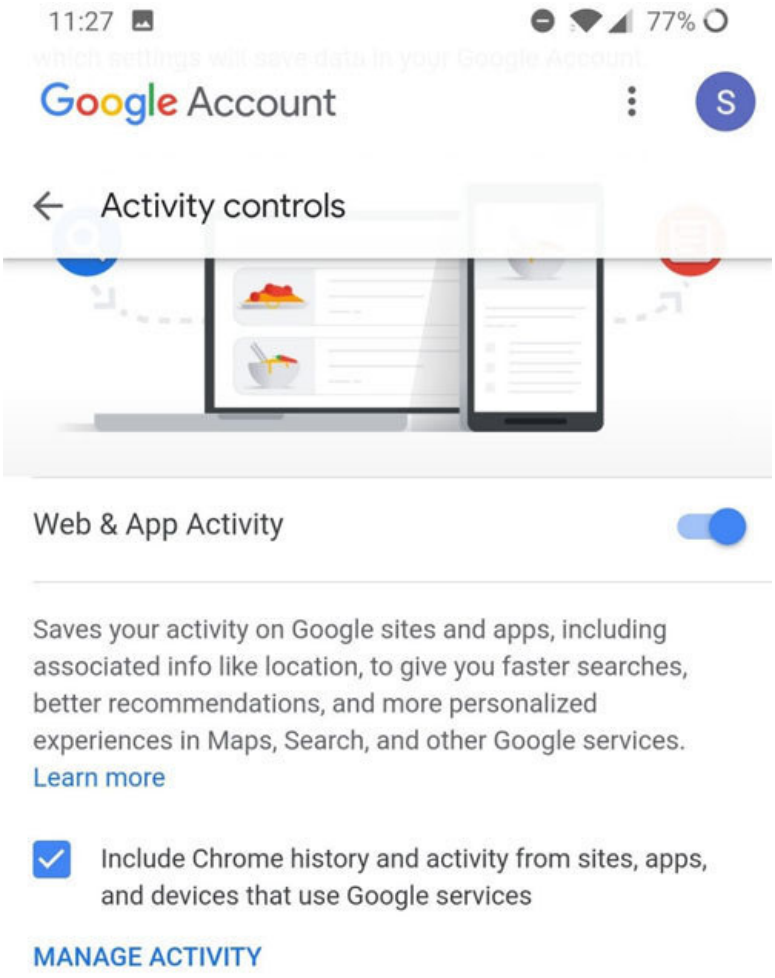


Figure 3.1: The "Activity Controls" section in a Google account accessed using an Android phone.

Alternatively, you can open your My Activity page in your Google account by going to:

https://myaccount.google.com/myactivity

Or, you can scan the QR code given alongside this paragraph and open; you're My Activity page using the browser app on your phone. Note that you may need to sign into your Google account before you can access this page in your browser.

BASIC: (1 point)

Each section describes the data that is being shared by your device with Google at any given point in time. Toggling any (or all) of the switches in the right to OFF will change the quality and amount of personalization that Google can provide -- sometimes even significantly -- thereby impacting your usage experience.

Click on the Learn More link in each of the sections to get a better idea of what data Google stores about you.

Next, disable as much of Google's tracking activity as possible, that is, toggle only those switches on that you absolutely cannot do without, to the OFF position.

Google will still maintain some anonymized info about you but toggling these switches will at least limit the amount of information they will be able to use.

INTERMEDIATE: (2 points)

There's still the matter of the data that Google has already collected about you. You also know that Google has already collected vast amounts of historical location data, web search and app usage data, device information, voice and audio activity, and even your YouTube watch history!

You can see all the data collected and stored by Google by going to:

https://myactivity.google.com/myactivity

Alternatively, scan the QR code shown alongside this paragraph and open the My Activity section of your Google account, using the browser app on your phone.

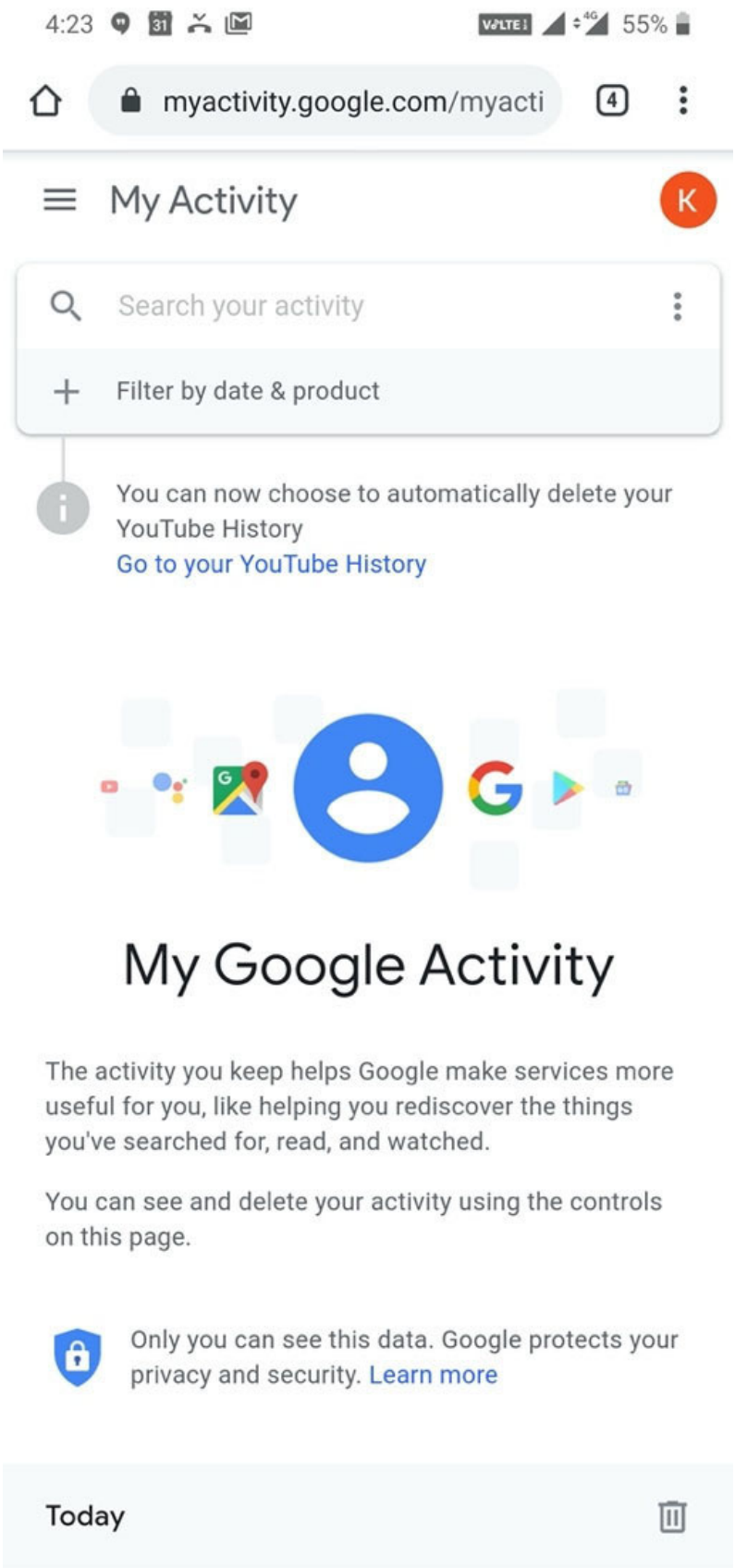


Figure 3.2: The "My Activity" section in a Google account accessed using an Android phone.

Click the link that says Delete Activity by , then under the Delete by date section, select All time in the dropdown, and click Delete . Read the confirmation dialog that appears, and then click on Delete again.

Click on the link that says Other Google Activity and, one-by-one, choose which activities you want to delete and delete them. Scroll down to the section titled Other Activity .

Choosing to follow this recommendation means that your internet experience will change -- somewhat or significantly – depending on which of the switches you toggled OFF . For instance, you might find that switching the Web & App Activity to off and deleting your activity data will result in severely limiting the functionality of Google Assistant.

Note that this does not delete the data from Google's servers; it merely prevents Google from using it to personalize your experience .

ADVANCED: (3 points)

For the more advanced users, I'd recommend blocking telemetry information from being sent out from your device. The two methods described below are merely popular examples; a little research on the internet will yield various other options that might prove suitable for your own unique situation.

Consider installing a more powerful adblocker like AdAway or Blokada on your phone. Both AdAway and Blokada rely on lists of known ad-servers and block all requests made to them. While Blokada accomplishes this by installing a 'local' VPN on your device, AdAway downloads the lists as a host file and, therefore, requires root.

Root your phone, and install a device-appropriate custom ROM that is known to be privacy-aware, such as Lineage OS, Una OS, or Replicant. A quick search on the XDA forums will reveal other options suitable for your Android device.

EXPERT: (5 points)

At this level, you might be required to invest some significant resources -- in terms of both money and time -- to ensure the privacy of your personal data:

If you must use an Android phone, do seriously consider switching to more privacy-aware alternatives, such as the SilentCircle BlackPhone2 and UnaOS. The Apple iPhone is also a viable option that is certainly worth considering.

It is possible to use Android without installing *any* Google services. However, this requires a significant amount of technical expertise and know-how and we absolutely, positively, comprehensively recommend that you DO NOT do this on your own. We strongly recommend consulting with experts if you want to set up and use your Android phone without Google services.

Important!!

Message From My Lawyer: If you still want to give it a shot, refer to Chapter 15: Set up your Android WITHOUT Google services. Once again, I do NOT recommend doing this without expert consultation. Should you decide to proceed, you will be doing so at your own risk, and neither the publisher of this book nor I shall be held liable should anything go wrong during the process. For once, I agree with him (my lawyer, that is) whole-heartedly!

Non-Google Telemetry

As I said earlier, Google isn't the only company that has access to your device and is interested in your data -- your device manufacturer is looking for ways to get a hold of that data too!

If you've followed either of the two recommendations under ADVANCED , then you are already set - nothing to do here. If you haven't or are looking for alternative recommendations, then I suggest you follow the recommendations listed below.

BASIC: (1 point)

If you don't own a device that runs stock Android, then I strongly recommend following these recommendations to opt-out of intrusive telemetry and unwanted advertising by various manufacturers - specifically OnePlus and Xiaomi.

OnePlus: To opt-out of the OnePlus device User Experience Program , open the Settings app, scroll down to System . You'll find multiple checkboxes under Experience improvement programs that you can toggle OFF right away.

Xiaomi: Someone over at XDA forumswrote a great post titled, Ads in MIUI 10 hamper the experience on otherwise great hardware: Here's how to fix them. It does a pretty good job of detailing how to get rid of recommended apps and ads on most Xiaomi smartphones. You can read it here: https://www.xda-developers.com/xiaomi-miui-ads-hamper-user-experience/

Scan the QR code given alongside this paragraph to read the post on your phone.

Others: For most phones, the telemetry options can usually be found in the Settings app under the section titled System or whatever is the appropriate equivalent for your device. If you don't find it in your phone, then either your phone doesn't have a telemetry program or doesn't advertise its telemetry.

Sensors

In Android, toggles for various sensors are almost always available via the Notifications drop-down. Note that switching off the sensors means that manual intervention will be needed at a later time.

For instance, turning off the GPS/Location sensor also means that Find my Phone service on your Android will not work as effectively since it can't accurately locate your phone. Apps that rely on location data (such as Maps, Uber, Ola, and more.) won't work until you turn the GPS/Location sensor on.

Similarly, you will need to manually turn on the Bluetooth sensor to connect to your car stereo or your Bluetooth speaker at home. You will need to toggle your Wi-Fi and mobile data when you move in and out of range and so on.

BASIC: (1 point)

Here's a quick guide on how to disable the various sensors on your device:

Swipe down to pull the Notifications screen. Swipe down again to expand the row into a grid:

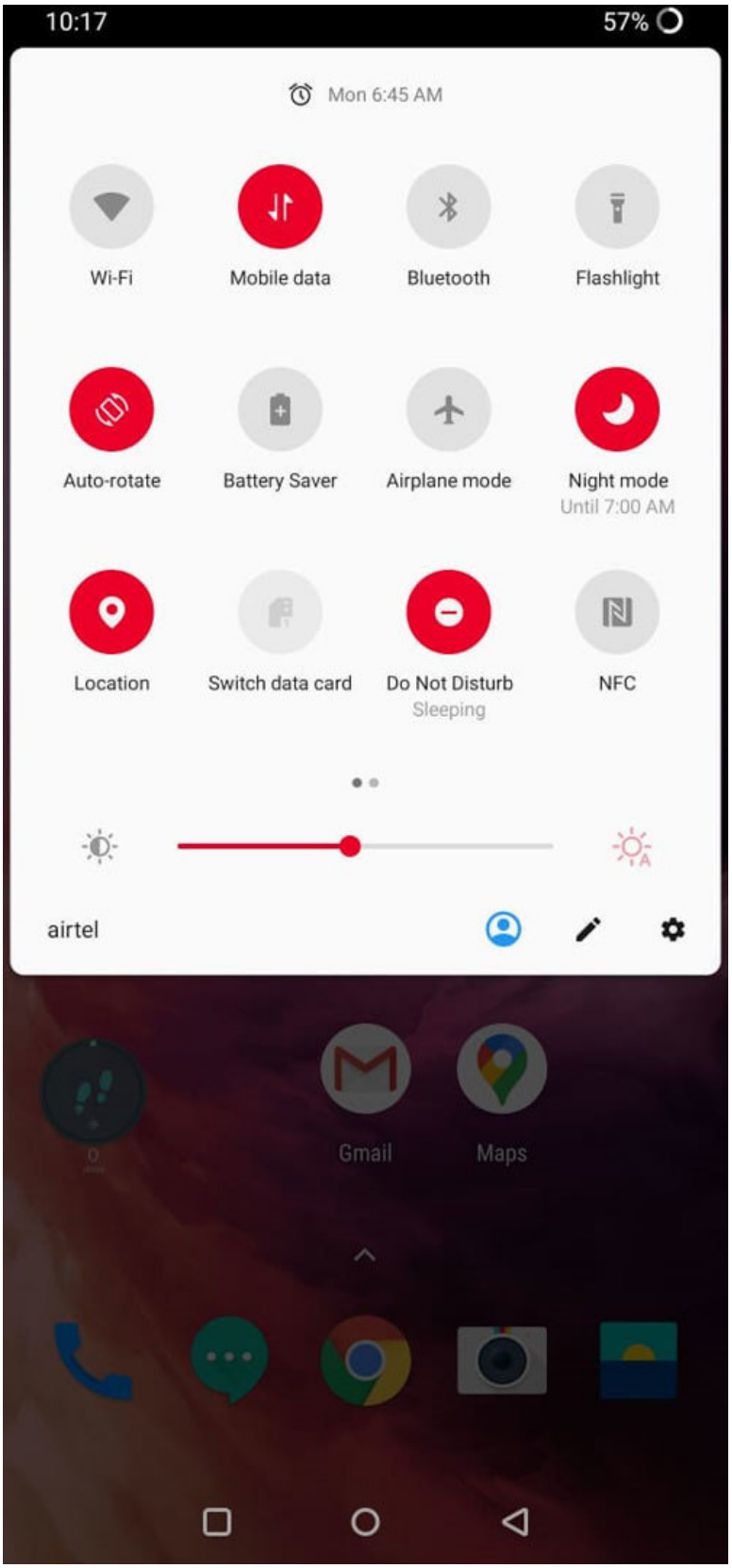


Figure 3.3: Accessing the notifications screen on a typical Android phone.

Locate the various icons for different sensors present in your device. Alternatively, open the Settings app on your phone.

Switch on only one of Wi-Fi or Mobile Data -- keep the other switched off.

Keep all the other sensors - GPS, Bluetooth, and NFC - switched off. If you don't see the GPS sensor toggle switch, look for an icon named Location instead.

Hint

If you don’t see all sensors, look for a small pencil icon that allows you to edit the icons in the notification grid. Perform the necessary actions to make these icons ‘active’ and bring up the Notification grid again.

Since these sensors consume quite a bit of battery, as an added bonus, switching off these sensors will help prolong your battery life as well!

Permissions

Starting with Android 6.0 Marshmallow, Google introduced the runtime permissions model for users to manage the permissions being given to various apps directly at runtime. What this means is, regardless of what permissions the app asks for during install, the dangerous protection-level permissions will be explicitly requested from the user by the app when the app is opened.

BASIC: (1 point)

I've already explained how the various app permissions available for Android apps affect your privacy. The minimum you should do knows the different permissions that each one of your apps has been granted.

This is actually quite easy to do because Android provides a nice interface to view all your apps categorized by the permissions granted to them.

In your Settings app, click Apps & Notifications , and then click App Permissions or whatever is the equivalent [6] for your device. If you did it right, you should be looking at something similar to the following screen:

Figure 3.4: The "Permissions" screen under the Apps section of the "Settings" app on your Androidphone.

Drill down into each of the permissions listed here and make a note of the various apps that have been granted this permission. The toggle switch next to each app indicates whether the app has been granted or denied specific permission:

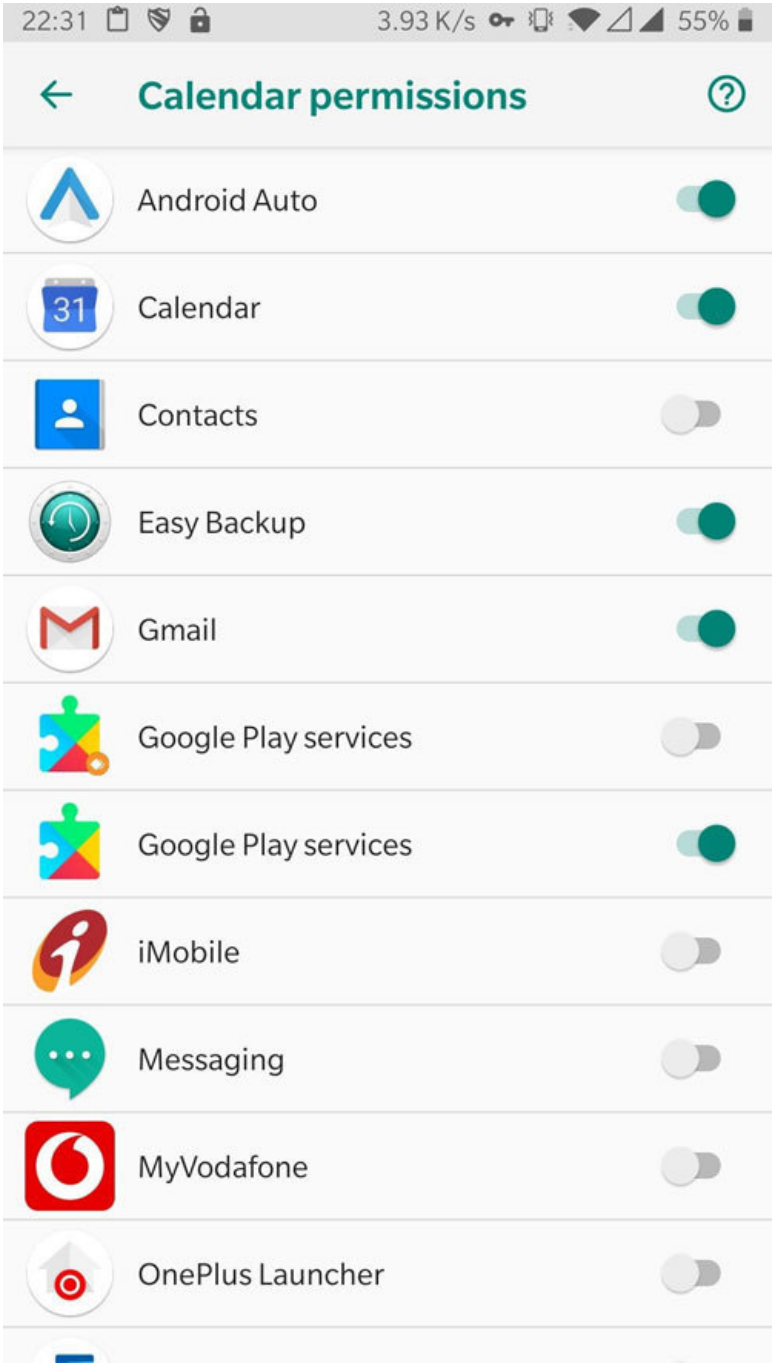


Figure 3.5: Drilling down into the Calendar permission in the "App permissions" screen.

Look for any apps that seem to have permissions inconsistent with their usage; for example, a Flashlight app shouldn't be given the Location permission. Refer to the Appendix (A) for a quick explanation for the various 'dangerous' permissions, if you wish.

Info

Importance of reviewing app permissions

If, at any point, you were wondering whether drilling down these permission groups was a waste of time, let me remind you what Facebook and Uber did a few years ago.

In 2016, Uber updated their app always to track the user's location, that is, collect location data in the background, from previously only collecting the data while the app was in use. In 2014, Uber was discovered to have implemented a real-time aerial tracking system called God View that used personal information to identify and track riders. In 2011, Facebook settled with the Federal Trade Commission and agreed to undergo an independent privacy evaluation every other year for 20 years over charges that it didn't keep its privacy promise to users by allowing private information to be made public without warning.

You might feel like you can trust behemoths like Facebook and Uber with your data, but these behemoths are as vulnerable to hacking attempts and data leaks as anyone else out there. For example, in 2013, Facebook disclosed details of a bug that exposed the personal details of six million accounts over approximately a year. Uber concealed a massive global breach of the personal information of 57 million customers and drivers in October 2016.

In a world where no one can guarantee the security of your data, wouldn't it be prudent to share as little data with anyone -- especially, these behemoths -- as possible?

INTERMEDIATE: (2 points)

Now that you've checked out the various permissions that apps on your phone have been granted, it is time to toggle a few switches!

Using your discretion, toggle the switch next to each app under each permission category to grant or deny that permission to the app. Don't worry; in most cases, the app will simply ask you for that permission again the next time you open it -- just remember to deny it when that happens.

For core Android apps that absolutely need certain permissions, (for example, the Contacts permission for the Phone/Dialer app) Android will display a warning dialog to inform you that, if you deny this permission, basic features of your device may no longer function as intended. It is usually a good idea to avoid the Deny Anyway option, and press Cancel in such situations.

Info

Google Play Services & Permissions

As you drill down into each permission category, you'll realize that Google Play Services appears in each one of them. That's because Google Play Services acts as a service provider (kind of like a trust-broker) for other apps on your device.

Many apps access data for performing various functions. For instance, Maps and cab-aggregator apps like Uber and Ola need the GPS/location permission to carry out their functions. Instead of requesting this information directly from the sensors, apps may then choose to request this information from Google Play Services.

Google Play Services, therefore, requests all permissions so that it can aggregate all necessary data from your device and provide it to any apps that may ask for it.

If you choose to deny permissions to Google Play Services, all you're doing is essentially declaring that you do not want Google Play Services to be a centralized provider of this data to apps on your phone. You are essentially stating that you want each app to request specific permission and not rely on Google to provide them with that data.

Most popular apps are well-designed and are programmed to handle this transition gracefully. However, you might find that some apps will not function properly after you choose to Deny Anyway for Google Play Services. This is because the apps rely solely on Google Play Services to provide them with that data.

You may also find that this change is *not* instantaneous; instead, apps will complain (or sometimes even crash) the *next* time you try to open them. When that happens, you will have two options: You can either decide to continue using these apps, or try and find suitable replacements for them.

Conclusion

Looking at Google's huge presence on the internet, it would be silly to assume that you can escape being tracked by them. The most you can do is severely limit the information that Google can acquire about you. To do this, however, would require entirely giving up on many of Google's excellent services such as Android, Gmail, and Maps, to name just a few.

Now, to be fair, some really good alternatives to all of these services exist and can be found across the internet. For instance, you could flash your Android phone with Lineage OS, use Protonmail and OpenStreetMaps instead of the native Google apps. However, this would mean that you'd be losing out on the inter-operability of its services -- one of Google's biggest advantages, which also happens to be a huge pain-point for privacy-enthusiasts like us.

In other words, finding suitable alternatives that will help reduce your dependence on Google (and its varied offerings) is a long and painful process. It is likely that you won't be able to achieve it all in one day. It is also likely that you won't be able to achieve complete independence from Google and its offerings.

I suppose that's the beauty of it, though. Ultimately, YOU get to choose how much you want to reduce your Google footprint.

---

[1] Yes, yes, I know Windows phones aren’t sold anymore. Microsoft announced in January 2019 that support for Windows 10 Mobile would end on December 10, 2019.

[2] The Windows phone has a significantly smaller market-share as compared to these two behemoths of the phone OS market, so we won't include them in discussions in this book. Windows phone enthusiasts are welcome to ask me their questions by emailing their questions at discuss@privacy.clinic

[3] There is a way to install Android OS on your phone without using any Google services. I've touched upon it briefly in a bonus chapter at the end of the book.

[4] I am not trying to target any manufacturer specifically here. I have simply provided these examples as a way to show how things can go massively wrong, regardless of how well-intentioned they seem.

[5] On Android versions before 6.0 Marshmallow, apps are granted the necessary permissions during installation itself. According to the Distribution Dashboard on android.com, that's about 25% of all Android phones in the market, as of July 2019.

[6] The exact name of the section may differ from phone to phone but the word 'permissions' will be mentioned somewhere, for sure.

Chapter 4

Apple iPhones

Introduction

The first Apple iPhone was demonstrated to the world by a very proud Steve Jobs at Macworld 2007—a trade show dedicated to all things Apple since 1985. From the moment he first spoke about combining the iPod, the phone, and the internet into one single device, the audience was hooked, and, in that moment, the world had changed.

Since that memorable day in January 2007, Apple has sold altogether about 1.5 billion iPhones worldwide. Furthermore, Apple has consistently been among the top 3 vendors in terms of the number of smartphone units sold in the last 5 years. iPhone sales have consistently accounted for more than half of Apple's total global revenue year after year.

Apple's stock has greatly benefited from the popularity of the iPhone, growing from just under $2 in 2001 to over $200 in 2019—a massive growth of over 15,000% in 18 years!! Apple also became the first publicly traded American company to have a net worth of over $1 trillion, making Steve Jobs one of the richest people in the world, at the time.

Most of Apple's success can be ascribed to the following three factors:

Premium branding: Apple iPhones are typically sold at a much higher price than most Android phones available in the market, making the iPhone a premium product. Not only does it help Apple's bottom-line, it also provides a sense of elevated status for the customer, thus making the whole deal a win-win for both parties.

Usability and design: Apple iPhones are designed with the average user in mind. While great care is taken to make the product look sexy [1] , Apple also ensures that the product by itself is easy-to-use by making its core functions extremely intuitive in terms of user experience.

Leadership thru innovation: Apple has been known to introduce and/or adopt various innovations that have later become industry standards. For instance, touchscreen devices existed before the iPhone, but the iPhone was the first touchscreen device that was deemed easy-to-use due to the simple-but-elegant interface accompanying it, viz. iOS.

In the last chapter, we compared Android phones to custom-built cars, all running the same engine viz. AOSP, but different peripherals and livery. We explained that Google Pixel, in the context of this analogy, was the phone equivalent of a stock car.

The Apple iPhone, too, is the phone equivalent of a stock car– except that every part of this stock car is made [2] by the same manufacturer, viz. Apple. In this analogy, iOS is the engine, the apps arethe essential car parts, the handset is the chassis, and Apple designs and manufactures all of them under its own brand. Furthermore, since they have established themselves as a premium brand, Apple iPhones are usually available at a premium as compared to Android Phones.

In this chapter, I will attempt to answer the question: From a security and privacy perspective, is it worth [3] paying the premium to Apple for their iPhone and/or other mobile devices such as the iPad?

The Apple Ecosystem

Apple's ecosystem is what people in the business describe as closed , that is, non-Apple employees do not get to see, much less modify, the hardware or the code that runs on these devices. Developers who wish to publish third-party apps on the iTunes store must pay Apple a license fee AND adhere to Apple's strict guidelines.

Being a closed ecosystem does have some advantages, though.

One, inherent weaknesses in such proprietary systems get automatically hidden along with everything else. This method, typically called 'security through obscurity', is useful in deterring malicious actors from breaching the system, since they can't know what weaknesses to look for. Two, a closed ecosystem can be well-regulated through rigorous checks and balances, due to its (relatively) small scope. All contributors to the system are clearly identified and any errors (or malicious activity) in the system can be quickly traced to the source.

However, closed ecosystems can still be vulnerable. The most common (and famous) example, in the case of Apple, is the concept of jailbreaking your iPhone, which I will discuss in greater detail a little later in the chapter.

iOS

Unlike Google and Android, all Apple iPhones run the same operating system—iOS. iOS is a proprietary Unix-like operating system that is specifically optimized for running on Apple iPhones.

iOS is one of the most uniformly updated operating systems in the smartphone market. As of August 2019, 88% of all iOS-based Apple devices (that is, iPhones and iPads) that are actively in use have the latest version of iOS, that is, iOS 12, installed on them (source: https://developer.apple.com/support/app-store/). If you also count iOS 11 in the mix, the number goes as high as 95% of all eligible devices!

Apple usually also ensures that a majority of its older devices are compatible with the newer versions of iOS. For instance, iOS 13 is available for device models iPhone 6s and later, while iOS 12 and 11 can be installed on device models iPhone 5s and upwards.

In other words, (almost) all Apple iOS devices will (almost always) have the same interface, although the underlying hardware powering them may be very different.

Info

Since almost all iPhones run the same version of iOS, they provide a consistent interface for users across different device models, both old and new.

However, it also means that 95% of all iPhones share the same attack surface – the iOS 12 and iOS 11 software code. Therefore, any vulnerability found in either of these two operating system versions affects (almost) every iPhone out there in the world.

This scenario becomes even more horrifying if you consider that there may be unknown vulnerabilities (commonly referred to as zero-day exploits) being actively exploited by malicious actors to conduct unauthorized breaches of data.

iCloud

Along with its devices, Apple offers the iCloud cloud computing and cloud storage service to all Apple users, estimated to be around 850 million users as of 2018.

Users can wirelessly backup all kinds of data such as documents, photos, and music to remote servers and sync them across various Apple devices signed into the same iCloud account using iTunes. The multitude of features offered by iCloud (For example, Collaboration, Sync, Backup and Restore, Family Sharing, and more), combined with multi-factor authentication, certainly make it an option worth considering.

I'd like to mention here that iCloud does not use end-to-end encryption but, in their privacy policy, they mention that they take precautions—including administrative, technical, and physical measures—to safeguard your personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction.

Info

In 2014, extremely private photos stored in the iCloud accounts of several celebrities were anonymously posted to the imageboard 4chan, and later spread to imgur and reddit.

It was initially believed that the hackers managed to gain access through vulnerabilities in some Apple services viz. Find My Phone and iCloud itself. Apple, however, denied any insecurity in iCloud itself and claimed that the celebrities were spear-phished, that is, their account credentials were acquired through a highly targeted attack by malicious actors pretending to be from Apple.

Regardless of who was actually at fault, the fact remains that the personal photos of a bunch of individuals were accessed by someone who wasn't authorized to access them. They were accessed from a secondary location, the credentials to which were acquired through illegitimate means.

Jailbreaking

To put it in the simplest terms, 'jailbreaking' an iPhone is similar to 'rooting' your Android phone, but the motivations and scope of these actions is very different. In both cases, you (somewhat illegitimately) gain complete control over your phones but both actions can also render your phone

vulnerable to malicious actions.

The act of jailbreaking usually involves exploiting vulnerability—either in the operating system code, or within the device hardware—to gain privileges as an administrative account or 'root' on the device.

Jailbreaking has several advantages from the end-user perspective:

Third-party apps: Apps that are unavailable through the official App store can be installed on jailbroken devices. This may include apps that have been banned, removed, deleted, rejected, or generally censored by the official App store.

Tweaks: Several unofficial tweaks and customizations are made by third-party developers, which can drastically alter the interface of your iPhone.

Unlocking: Carrier-locked and region-locked iPhones can be unlocked and used with other carriers and in other regions.

Privacy: Control the uploading of telemetry and usage statistics to Apple servers.

However, from a security perspective, jailbreaking can introduce some serious vulnerabilities on your iPhone:

Piracy: The most common reason for jailbreaking iPhones is to circumvent the official App Store and install pirated apps.

Malware: Malicious actors often install malware and tracking software on jailbroken devices.

Worm: An insecure SSH service on jailbroken devices can allow an attacker to gain entry onto your device and compromise your device usage.

Info

In November 2009, an Australian student created the first iPhone worm called iKee based on this insecure SSH service exploit to raise awareness about security issues around jailbreaking.

The same month, the Finnish cybersecurity and privacy company F-Secure reported the discovery of a new malicious worm that compromised bank transactions on jailbroken iPhones in Netherlands.

In August 2015, a malware named KeyRaider was discovered that was believed to have stolen the login credentials of more than 2 lakh users, affecting only jailbroken devices. KeyRaider was said to have affected users who downloaded apps from the Cydia app repository.

Since users with jailbroken iPhones are more vulnerable than regular iPhone users, and more likely to install pirated apps, it is in Apple's interest to pro-actively patch any vulnerabilities that can be used to jailbreak iPhones. Therefore, Apple actively releases various software patches for iOS to close down any and all jail-break vulnerabilities that are found. This why most jailbreaking software end up disabling OTA updates to ensure that users don't accidentally install these patches released by Apple.

However, if there happens to be a bootroom exploit, that is, an exploit found in the hardware of the device, it cannot be patched, unless you upgrade to a newer handset with newer hardware that does not contain the exploit. For instance, in September 2019, a bootroom exploit called checkm8 [4] (pronounced: checkmate) was discovered that affected all iPhone models upto and including iPhone X.

Opinion

I'm not explicitly trying to say that jailbreaking is inherently evil or jailbreaking is chaotically good. In fact, I do not have an opinion either way on the matter.

Legally speaking, jailbreaking is a violation of Apple's ToS and you shouldn't do it. However, jailbreaking also forms a significant part of the Right to Repair movement, if you believe in that sort of thing.

At the end of the day, jailbreaking, like rooting, is a highly advanced and technical thing to do to our iPhone. All I'm saying is that it deserves to be done with the greatest respect and utmost care.

Apple and Privacy

The biggest difference that sets Apple apart from Google is the way they treat user data. While Android has been known to (rather aggressively) collect all kinds of data from its users, Apple has labelled itself a product company and strongly distanced itself from any and all data-collecting activities.

In fact, Apple CEO, Tim Cook, explicitly stated in a May 2019 interview with ABC that Apple "has no interest in collecting users' data" because that's not their product, as they are in the business of selling devices. "You are not our product," he said. "Our products are iPhones and iPads. We treasure your data. We wanna help you keep it private and keep it safe."

If you think that means Apple does not collect any data from its users, you'd be very, very mistaken.

Apple definitely collects quite a bit of usage data from all Apple devices, except they claim that they only collect usage data, and not data stored on the device. Furthermore, even the data they collect is anonymized, (mostly) opt-in, and only collected to help improve their services, under the Differential Privacy [5] policy.

Note

Apple's Differential Privacy Policy

Scan the QR code displayed alongside to download the Differential Privacy Overview PDF, which details the various techniques used by Apple to anonymize the data and the particular steps taken to ensure that the privacy of the user (and their data) remains protected.

[QR Code: https://www.apple.com/privacy/docs/Differential*Privacy*Overview.pdf]

Fortunately, Apple does make it (relatively) easy to opt-out of this data-collection. I'll explain how to opt-out of Apple's data-collection in detail, in the #RohitRecommends section towards the end of this chapter.

Sensors

Like all modern smartphones, all Apple iPhones come equipped with several sensors and radios that perform various important functions on your device. Along with the standard WiFi, GSM, and Bluetooth sensors, most modern iPhones also come equipped with Near-Field Communication, or NFC, chips to make payments using your iPhone possible. The latest iPhone (iPhone 11) also incorporates an Ultra-Wideband chip for spatial awareness.

Along with these standard radios , most modern iPhones (6 and upwards) also have several sensors that provide specific enhancements to your iPhone usage. For instance, proximity sensor, ambient light sensor, gyroscope, compass, barometer, Touch ID, and more.

Whenever active, these sensors and radios may share data in real-time with apps that might request them for their data, provided you grant them the necessary permissions for doing so.

While this seems to be a fairly trivial and seamless operation, I'd like to remind you once again that I've already described and demonstrated how these sensors can inadvertently leak data.

Therefore, as with Android, I would strongly urge you to keep your sensors switched off/deactivated until you legitimately need to use them, and then switch them off/deactivate them again when you are done. The details on how to achieve this are provided under the # RohitRecommends section at the end of this chapter.

Permissions

Permissions refer to the requests made by an app to access the user's personal data on the device. These usually appear as floating dialog boxes whenever the app finds it necessary to request that permission.

Just like Android, Apple also allows granular permission control over the apps you install on your iPhone. When apps are installed on an iPhone, they are not granted any permission by default. All apps *must* acquire explicit permission from the user before accessing any private information on the device. These permissions are requested only as and when necessary. However, the permission granted is perpetual; although, you can modify or revoke these permissions anytime.

Unlike Android, Apple provides an additional level of granularity for the Location permission, where you can choose the Frequency with which GPS and location data is shared with the apps that request it. Apple provides three frequency-levels of access to GPS/location data: Always , While Using , and Never , which I am assuming are self-explanatory.

I would strongly recommend that you allow apps to access your GPS/location data only While Using . This will ensure that apps do not accidentally leak this information to any third-parties without your knowledge.

The Settings App

One of the things that is different about Apple is the fact that all the important privacy settings and access permissions pertaining to every app

installed on your iPhone are available under the corresponding sectionin the Settings app.

If you click on the section corresponding to an installed app, you can (usually)definitely find the following subsections:

Permissions: The various permissions that were requested by (and granted to) the app. You can drill down further and either selectively revise or entirely revoke these permissions.

Siri & Search: The toggle switches under this subsection allow various kinds of information from the app to appear in results provided by Siri and related search functions.

Optionally, the following sub-sections may also be present for some apps:

Background Refresh: This is a toggle switch that determines whether the app is allowed to perform its operations in the background, even when it is suspended.

App-specific settings: Each app may have its own set of settings for the user to modify.

Note that each app uses a different approach to populating their respective section under the Settings app. In some cases, this subsection may be completely empty for some apps (except for the Permissions subsection and the Siri & Search subsection), but there may be an entirely separate Settings page within the app itself.

Analytics and Advertising

Compared to Google, Apple seems to take its stance on user privacy rather seriously. On its website, through various articles and support documents, Apple provides a rather transparent (and quite detailed) explanation about why and how it collects your data and what it does with that data.

I must admit, Apple seems to have gone out of its way to explicitly detail the various kinds (and amounts) of data it collects, on its website.

However, don't let this distract you from the fact that, if left alone and if left without intervention, Apple is likely to collect a bunch of data about (and from) your iPhone. I mean, for all the claims that Apple makes about being in the business of selling hardware and not your personal data, the fact is that it also sells ads through the Apple's Ad Platform. According to the support page detailing the Apple Advertising and Privacy policy:

Ads that are delivered by Apple's advertising platform may appear on the App Store, Apple News, and Stocks.

Scan the QR code displayed alongside this paragraph to check out the Apple Advertising and Privacy support page. If you have the time and curiosity, I recommend that you read it – won't take you more than 10 mins, I think.

[QR Code: https://support.apple.com/en-us/HT205223]

Note

TL; DR for Apple's Advertising and privacy support document/page

If you are curious about what it says but are also lazy enough that you can't be bothered to scan the QR code, consider the following a quick, short primer on what the Apple Advertising and Privacy support page is all about.

Apple collects information pertaining to your device and usage, viz. keyboard language, device type, OS version, mobile carrier, connection type, device location, the searches you perform on the App Store, and the types of articles you read.

Apple creates segments, that is, groups of people who share similar characteristics, based on some of this collected information. Targeted ads are shown only if a segment has more than 5000 people.

The segments are further augmented using other usage and account data, such as your name, age, gender, address, downloaded content and apps, previously viewed ads, and many more.

Advertisers may further augment any data provided by Apple by matching it with data (for example, email, phone number, and many more.) they may have independently collected from the end user. While Apple tries to obfuscate as much as it can, Advertisers still have access to the

Advertising Identifier, which they may use to categorize users into certain segments.

To explain it using a simple example, if less than 5000 people from your city search for music-streaming apps on the App Store using their iPhones, Apple will not show targeted ads from advertisers looking to target people interested in musicstreaming.

One thing that Apple makes abundantly clear is that they collect only usage data and not on-device data. Furthermore, they add random noise to this usage data so as to ensure that any personally identifiable information (PII) is overwritten and not directly accessible to the advertisers. Then, the data of several users is collected and separated into buckets of 5000 or more users. If a particular advertising category has less than 5000 users, the data is not made available to advertisers, thus reducing the possibility of fine-grained targeting of end users like you and me.

However, there is no end-to-end encryption involved, that is, the usage data that is transported to Apple's servers is not encrypted on the device, only during transit. Therefore, the possibility exists that a sufficiently motivated malicious actor could theoretically be able to access this data on your device.

Fortunately, Apple makes it rather easy to control what data is shared with Advertisers, in the Privacy section of your Settings app. You might not be able to stop it completely from collecting data, but you can definitely reduce the amount of data that gets collected. I'll discuss it in greater detail in the #RohitRecommends section of this chapter, of course.

RohitRecommends

Those of you who read the first chapter carefully must have realized immediately that (anonymized or not) Apple's Differential Privacy policy still violates the third principle of data-sharing, viz. If the data is encrypted, but not in your control, then it might be secure but it is not private.

Therefore, my recommendation would be to reject Apple's telemetry as much as possible by toggling the appropriate switches under the Privacy section in the Settings app. Be aware, however, that this might seriously change your device usage experience, since Apple does rely on this data to give you a somewhat personalized experience on your device.

For example, the keyboard and typing analytics that Apple collects from your device contains details about hardware and OS specs, performance stats, and selected usage data—all anonymized and scrambled before uploading to Apple's servers. Apple then utilizes this data to improve the intelligence and usability of features such as QuickType suggestions, Emoji suggestions, Lookup Hints, and many more.

Here's what you can do to keep your personal data private and out of Apple's reach.

iOS and iCloud

If you haven't checked to see what data from your iPhone is getting backed up to iCloud, now would be a good time to take stock.

Open the Settings app and scroll down to the section titled iCloud . If you don't find a section titled iCloud , look for the section with your name. Click to open this section.

Here, you'll find toggle switches corresponding to various services such as Calendar, Reminders, Safari, Notes, and many more. Services with switches that are toggled ON are being backed up to iCloud, and services with switches that are toggled OFF are not being backed up to iCloud.

Figure 4.1: Accessing the iCloud options under the Settings app on your iPhone.

You can choose to either selectively sync the various apps and services listed here or you can stop your iPhone from syncing with iCloud altogether. Before you do either of them, you need to understand what either option actually does.

Take a look at the list of apps and services that are syncing data with iCloud and ask yourself the following questions:

Do any of these apps contain (or are likely to contain) any personal information now or in the future?

If someone else were to gain access to the app's data, what would they see? Am I worried about them seeing it?

If an app (or multiple apps) crashed, and all information contained within got deleted right now, would it cause you massive and irreparable loss?

Did you answer Yes to two or more of these questions?

BASIC (1 point)

If you answered Yes to at least two questions, then maybe turning off iCloud syncing selectively on a per-app basis would serve you better than signing out of iCloud entirely.

Go through the list of questions and ask the question for each app. Then, depending on the answers, toggle the sync settings ON or OFF selectively for each app.

ADVANCED (3 points)

If you answered No to all three questions, then I strongly recommend you sign out of iCloud altogether. You can do this by scrolling down to the bottom and clicking Sign Out . This will stop your phone from syncing to iCloud entirely and none of your data will be automatically backed up.

Sensors

Just like Android, device sensors on your Apple iPhone can be toggled ON or OFF. In case of Wi-Fi, Bluetooth, and mobile radio, the toggle switches for the sensors can be accessed by swiping up on the home screen or from their respective sections in the Settings app. However, the option to turn off Location Services can be found under the Privacy section of the Settings app.

Toggling these sensors off restricts apps from accessing the sensor data. This might result in some apps working incorrectly or not at all. For instance, toggling the Bluetooth sensor off prevents your Phone from connecting to other Bluetooth devices such as your car stereo or wireless speaker. Apps and services that rely on Bluetooth, such as AirPlay or ShareIt, might also not work as effectively or properly.

Similarly, turning off the location sensor prevents mapping apps and ride-sharing apps (for example, Uber, Ola, and Lyft) from working effectively. The Find my Phone feature also requires location services to be turned on for it to work effectively.

That said, toggling these sensors off helps in two important ways:

It greatly helps your device conserve battery.

It reduces potential attack surfaces for any potential adversaries.

It is definitely a trade-off, and you need to decide whether you want to toggle the sensors OFF or if you want them to remain toggled ON. If you can't come to a decision, here's my recommendation: open your Settings app and look at each sensor that is currently toggled ON, and ask yourself the question:

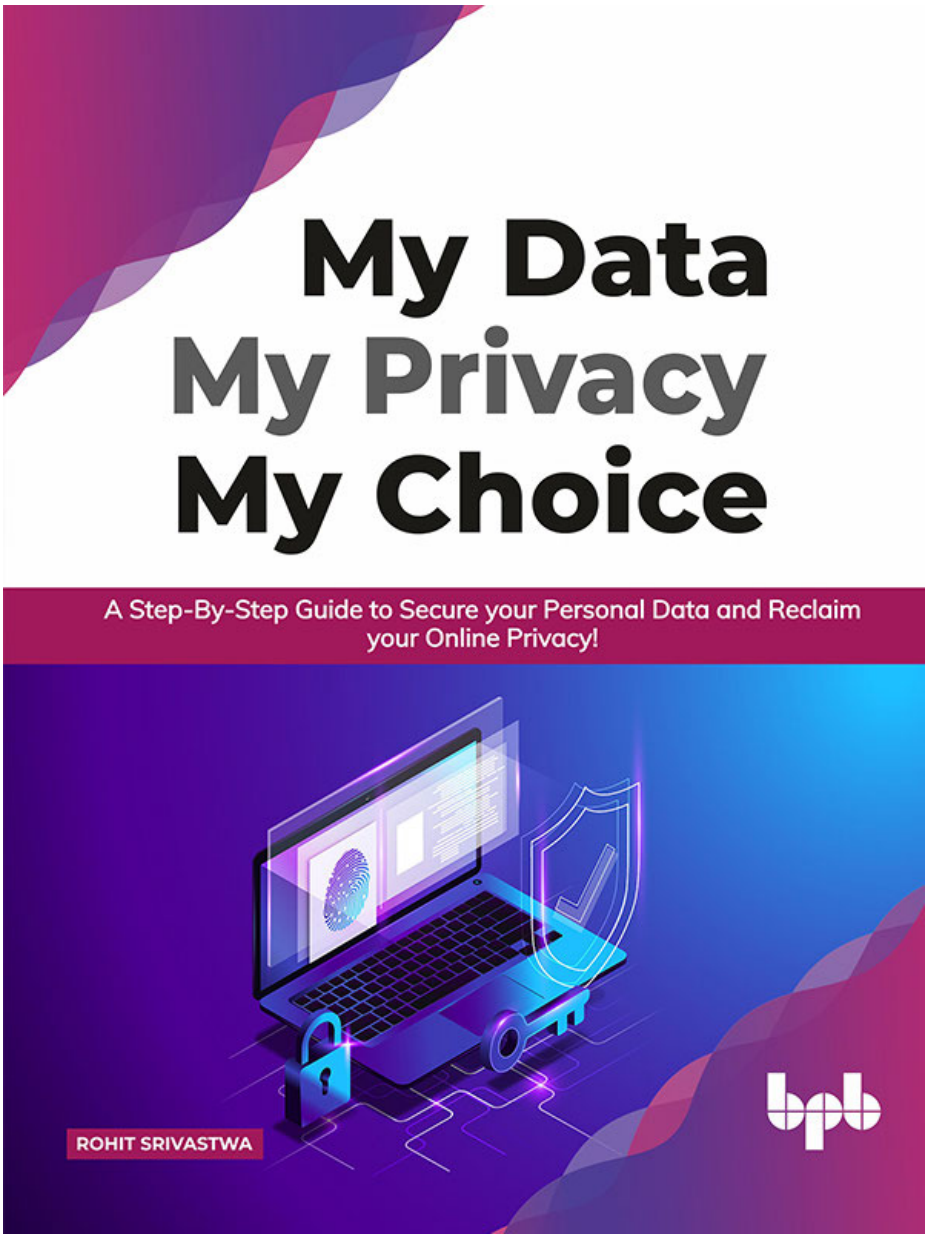
Is this sensor currently being actively used by an app?

Is the app being used (either actively or passively) by me?

BASIC (1 point)

If you answered Yes to both questions, then leave it be – just remember to toggle it OFF once you are done using the app that is using the sensor.

For example, I'd recommend that you toggle the location services off when you are not using the Maps app/service. Toggle Bluetooth off if you don't have any Bluetooth devices connected to your iPhone.



ADVANCED (3 points)

If you answered No to either or both questions, then I'd sincerely recommend that to toggle the sensors OFF .

For example, if you regularly carry your iPhone on your person, or if you are stationary (that is, at home or in the office), then keeping the Location Services toggled off will help you conserve your battery life. Similarly, I recommend that you toggle the Wi-Fi off when it is not being used, that is, when you step out of home or your office, for example.

My Data My Privacy

My Choice

Permissions

To modify or revoke permissions for an app, you can open the Settings app and either:

Scroll down and click on the section corresponding to the app.

Open the section titled Privacy and click on each permission sub-heading.

Like Android, Apple too provides easy access to toggle these permissions ON or OFF. The following image shows a screenshot displaying the various headings seen under the Privacy section in iOS 12.3.1.

A Step-by-Step Guide to Secure Your Personal

Data and Reclaim Your Online Privacy!

---

by

Rohit Srivastwa

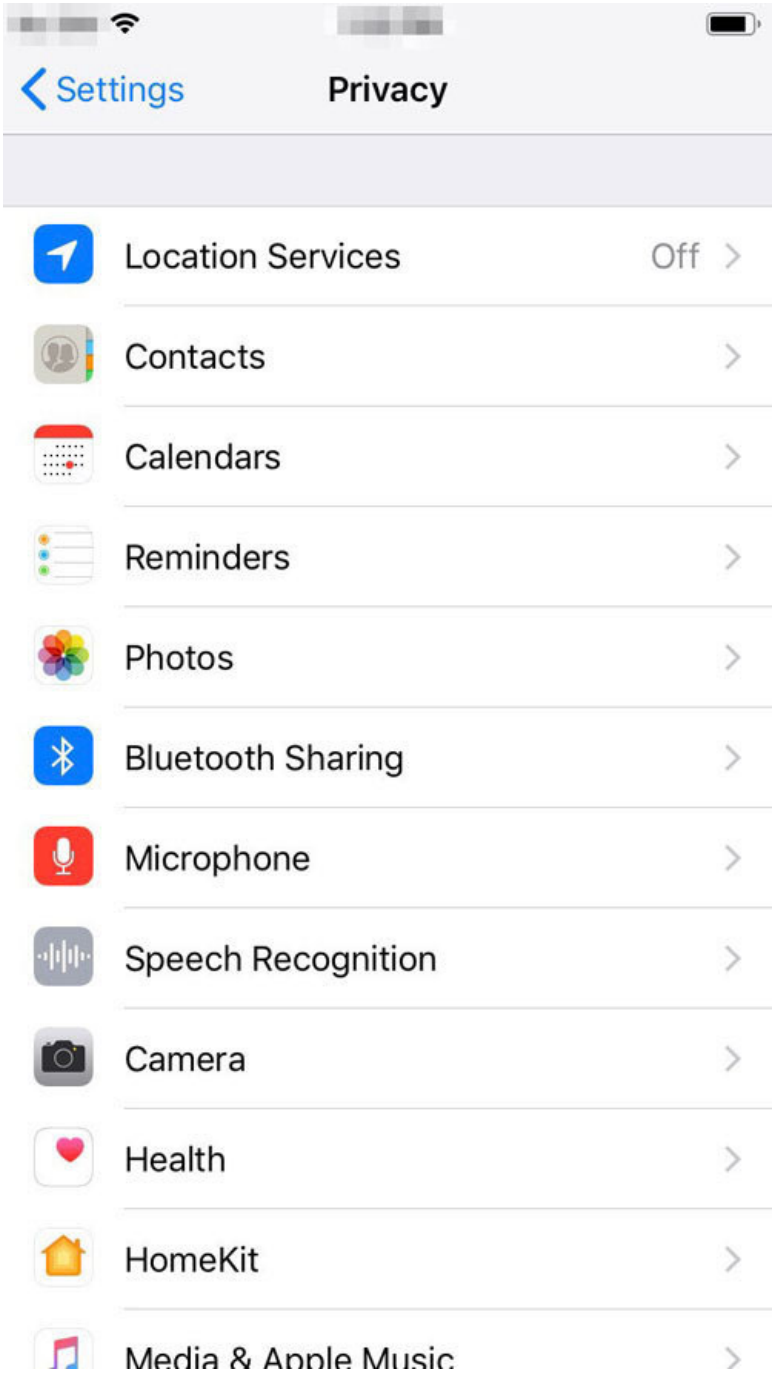


Figure 4.2: The 'Privacy' section in the “Settings” app seen on an iPhone 6s running iOS 12.

Like we did with sensors, we first need to understand which of these permissions are inconsistent with the app's usage before we can opt to modify or revoke them entirely. So, as you drill down into each permission sub-heading, ask yourself the following questions:

Is this permission absolutely necessary for this app to function?

Am I okay with this (permission-specific) data being shared with this app?

For the Location permission, am I okay with the frequency with which the app can access location data?

Once you have answered these questions, proceed to the next step to figure out which recommendations you might able to follow.

BASIC (1 point)

If you answered Yes to all the questions, then there isn't much to do here. You can skip the rest of the recommendations and safely proceed to the next section.

FIRST EDITION 2020

ISBN: 978-93-89845-181

Distributors:

BPB PUBLICATIONS

20, Ansari Road, Darya Ganj

New Delhi-110002

Ph: 23254990/23254991

MICRO MEDIA

Shop No. 5, Mahendra Chambers,

150 DN Rd. Next to Capital Cinema,

V.T. (C.S.T.) Station, MUMBAI-400 001

Ph: 22078296/22078297

DECCAN AGENCIES

4-3-329, Bank Street,

Hyderabad-500195

Ph: 24756967/24756400

BPB BOOK CENTRE

376 Old Lajpat Rai Market,

Delhi-110006

Ph: 23861747

Published by Manish Jain for BPB Publications, 20 Ansari Road, Darya Ganj, New Delhi-110002 and Printed by him at Repro India Ltd, Mumbai

ADVANCED (3 points)

If you answered No to any of the questions above, you might need to (re-)evaluate your use of the app and the permissions being granted to the app.

If the app can still function after being denied some permission, then you might want to try toggling it off and see how it impacts your usage of the app. If the data being shared with the app contains some very personal information, then you might want consider not using the app or using a different one.

The frequency only matters for the Location permission and, as I mentioned earlier, toggling it to While Using should be more than enough for most apps.

As an example, let's look at one of the most popular apps on the App Store—Instagram. By the time you set it up and use it regularly, Instagram will have requested for and (most likely, be granted access to) the Location, Photos, and Camera permissions.

The following image shows a screenshot of what the Instagram settings screen might look like on your iPhone after navigating these permission requests:

Dedicated to

Everyone who respects their privacy and wants to live a safe life online

Figure 4.3: To access this screen on your iPhone, go to Settings | Instagram

You'll notice that some permission such as Camera and Photos are absolutely necessary for the app to work. However, the Location permission is only required if you want to geo-tag your posts.

Here's the thing, even if you toggle the Location permission to Never , you'll still be able to geo-tag your posts by searching manually for the location before posting your photo to Instagram! Of course, this means you are now voluntarily sharing your location data with Instagram. However, this defeats the purpose of the whole exercise, viz. maintaining the privacy of you and your data, so I'd recommend against doing it.

Foreword

The COVID-19 pandemic has made “virtual,” the new reality, and we are now living in an age where the internet is no longer a novelty but a necessity. What began as a rather complicated way to send simple messages from one machine to another has now evolved into a behemoth that allows us to do all kinds of things – simple AND complicated – often, at the mere touch of a button. We have rapidly progressed from sending each other little packets of text to doing almost everything – communicating, shopping, relaxing, creating, sharing, spreading – on the internet.

However, this evolution has extracted a high cost from us. Every username and password combination that we create on the internet is a tiny peephole into our lives. The notion of privacy exists only as long as these peepholes remain unknown to outsiders. The more peepholes we create, the more vulnerable we make ourselves to all these outsiders, who will relish any opportunity to sneak a free peek into our lives.

Consider this, the website “Have I Been Pwned” (https://haveibeenpwned.com) contains a record of more than 9.5 billion accounts from 440 websites that were ‘hacked’ by miscreants. DeHashed (https://www.dehashed.com) contains 12.5 billion “compromised assets” from “all corners of the internet.”

There is a genuine chance that one of those accounts could belong to you. If you are the kind of person who reuses their password across multiple websites and doesn’t change passwords very often, then all your accounts are suddenly open to invasion. From merely having one leaked account, your entire online presence suddenly went under threat.

The early users of the internet merely had to contend with fundamental problems such as transmission and display of data. Today, the average internet user transmits several pieces of PII – personally identifiable information – to remote servers, often without realizing it. Were this information to get leaked or intercepted, it could represent a significant threat to our well-being. The need to ensure the security of our online identities and the privacy of our online data should, therefore, be considered paramount in this day and age.

That’s where Rohit Srivastwa’s years of expertise with cyber-security and digital privacy comes in handy. With his book, “My Data, My Privacy, My Choice,” Rohit offers a clear and well-laid path to extricate yourself out of the mess that is maintaining the privacy of your online identities.

Rohit guides you, the reader, carefully, with step-by-step instructions that take you from understanding the problem to solving the problem. The solutions (wonderfully named #RohitRecommends) are structured carefully in a four-tiered structure ranging from Basic to Expert, with each subsequent level providing a stronger layer of security and better privacy for your online identity. Each level of recommendation is self-sufficient (to a degree), and there is no compulsion to follow recommendations at a level that you find difficult to comprehend.

Rohit has also introduced a gamification framework to incentivize the adoption of these recommendations by assigning ‘points’ to each recommended action. As you go through the book, you collect points, and the final tally gives you an idea of your PrivacyScore. The higher the level of recommendations followed, the better your PrivacyScore will be.

Another unique aspect of the book is its interactive, cross-media capabilities. Instead of relegating relevant reading to the usual ‘References’ section, the book uses smartly-placed, contextual QR codes that you can scan to acquire additional knowledge of the subject without ever leaving the page of the book that you are on!

Rohit Srivastwa strives to make the subject of online privacy and cybersecurity easy to understand and implement for everyone. He has succeeded in creating a framework that makes it easy for everyone to implement a degree of control over their online data and reclaim their online privacy.

Lt. Gen Rajesh Pant, PVSM, AVSM, VSM (Retd.), PhD

National Cyber Security Coordinator - PMO

Govt of India, New Delhi

Settings | Privacy

Simply speaking, what Android calls dangerous permissions, Apple calls Privacy settings. These Privacy settings can be accessed by opening your Settings app and scrolling down to the section named Privacy . Tap on it to open it.

Broadly speaking, the headings under this section can be classified under the following five categories:

Location sensors: Options to toggle the Location Sensor ON or OFF.

Personal data (text): Contacts, Calendars, Reminders, and Bluetooth Sharing.

Personal data (non -text): Photo, Camera, and Microphone.

Smart devices : Home, Health, and Motion and Fitness.

Analytics and advertising: (self-explanatory).

The fundamental concepts behind these permissions are the same as that on Android. The names may be different but the ideas are very much the same. In fact, you might want to read the section in Chapter 15 , titled, “The 10 Android permissions listed under 'dangerous' protection-level” for a brief discussion of what these permissions mean and examples of typical/atypical apps that might request these permissions.

Testimonials

The thing about the internet is that it is a wonderful place, BUT there are some not-so-wonderful people on it…

“My Data, My Privacy, My Choice!” by Rohit Srivastwa makes it easy to explore the wonders of the internet while ensuring that you avoid bumping

into these not-so-wonderful people! I felt that the gamification of recommended actions (#RohitRecommends) ensured that I, as the reader, was substantially incentivized actually to follow the recommendations set out. By the end of the book, I could see a clear difference in my browsing habits, and I could *feel* my network traffic heaving a sigh of relief!

Rohit Srivastwa has written a superb guide with valuable information on every page written in easy-to-understand language. I highly recommend it for those who are looking to get started on the journey to securing their online identity and reclaiming the privacy of their digital data

- Brijesh Singh, IPS

Former Inspector General of Maharashtra Cyber

As our physical and digital world merge, we need to go in for certain lifestyle changes so as to protect ourselves from digital threats and safeguard our privacy continuously as technology shapes our every-day lives. While various learning platforms, scholarly articles on the internet, online courses, watching Youtube, podcasts, blogs, etc. can help create awareness and learning amongst us, however, it is an excellent book that is the best way to get in-depth knowledge which is the most helpful. With years of experience in the cybersecurity and privacy domain, Rohit Srivastwa, as a first-time author, has shared his in-depth knowledge in a clean, understandable, lucid, and practical manner. Rohit has cleverly weaved the concepts of gamification with the educational objective of making awareness and learning more appealing while motivating users by providing insightful suggestions neatly categorized into basic, intermediate, advanced, and expert - thus nudging you to improve your baseline continuously.

Pick up “My Data, My Privacy, My Choice” and take action today so that you can embark upon your digital adventure confidently and enjoy your journey!

- Dr. Sanjay Bahl, Director General

Indian Computer Emergency Response Team (CERT-In)

BASIC (1 point)

If you drill down into each of the sections one-by-one, you'll find a list of apps that have requested the corresponding permission. The toggle switch next to each app indicates whether or not the app has been granted that particular permission. If you change your mind after you grant permission, you can restrict (or entirely revoke) these permissions by toggling the switch next to a specific app, much like you would do in Android.

For instance, you may want to give location permissions to apps only While Using and not Always . Or you might want to revoke Facebook's access to your address book by toggling the switch next to Facebook under Settings | Privacy | Contacts to the OFF position.

About the Author

Analytics and Advertising

For what it's worth, Apple does provide a very easy method to turn off all Telemetry and Analytics for users who wish to opt-out of Apple's datacollection.

Open your Settings app, and scroll downto the section titled Privacy . Then, scroll all the way down to the bottom where you will see two subsections titled Analytics and Advertising .

The following image shows a screenshot of what the Analytics and Advertising Settings screen might look like on your iPhone:

Rohit Srivastwa is a serial entrepreneur, a recipient of Microsoft MVP award in the domain of “Enterprise Security,” and a multifaceted professional with experience in Cyber Security, Enterprise Security, Enterprise IT, Secure Digital Transformation and Cyberwarfare. He is also actively involved in advising several Military agencies, Law Enforcement, Corporate, and Government bodies of different countries in these fields.

He is a well-known Security Evangelist and Founder of India’s first-ever hackers’ conference and community named “ClubHack.” He has had a bunch of start-ups in the past, with the last one acquired by QuickHeal Technology Ltd in 2016.

A teacher at heart, Rohit has designed the entire MTech program in Information Security that is being currently offered by Pune University. He is

also a visiting faculty at several A-grade institutions such as IITs, IIMs, Symbiosis, etc. He is a liaison member at FIRST.org, where his responsibilities include liaising between CERTs of different countries and companies.

He has been featured in many technical shows and news panel discussion related to cyber warfare and cybersecurity. Rohit is also a renowned speaker and has spoken in many events across the globe, including TEDx, Microsoft Digital Crime Convention, among others.

Current Roles

Founder, ClubHack Labs

Virtual CISO, Various Large enterprises

Advisor, Science & Technology Park, Dept of Science & Technology, Govt of India

Mentor and Advisor, Several Cyber Security Start-ups

Charter Member, TiE

You can tweet the author @rohit11 and also follow his security and privacy recommendations on twitter using #RohitRecommends

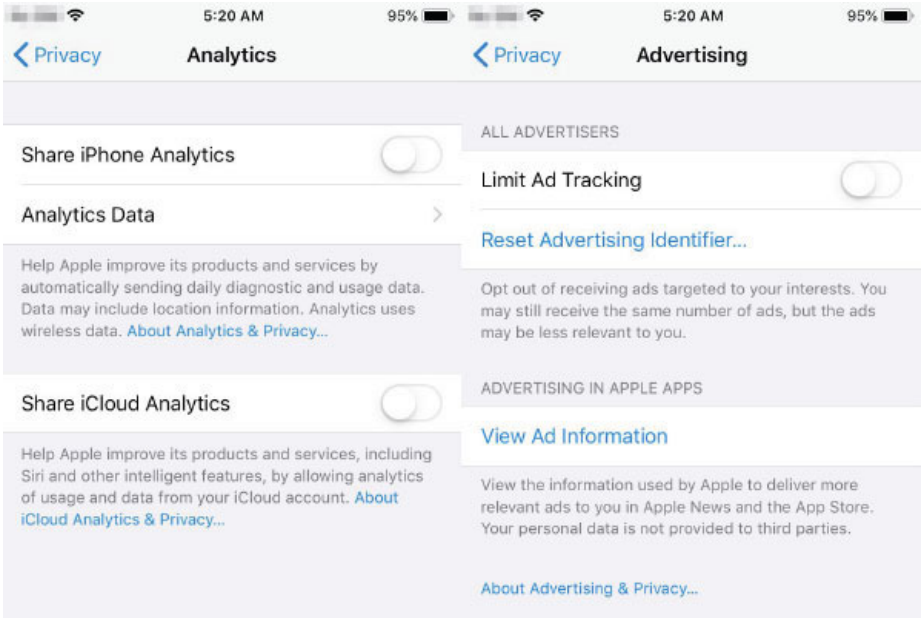


Figure 4.4: The Analytics and Advertising sections under Settings | Privacy.

The Analytics section allows Apple to collect your usage data on a daily basis, while Advertising refers to the data collected by Apple for targeted advertising, subject to the collection methods described earlier in this chapter. Here is a quick description of what you can expect to find under each of these sections:

Under the Analytics section, drilling down into Analytics Data shows you all the data that was sent to Apple. You can also read more about Apple's stance on data collection for analytics by clicking the link titled About Analytics & Privacy under the Analytics Data section.

Under the Advertising section, clicking on View Ad Information brings up a window with details on the information collected for targeted advertising from your device by Apple. You can also read more about Apple's stance on data collection for targeted advertising by clicking the link titled About Advertising & Privacy … at the bottom.

While Apple claims that none of the collected information identifies you personally, I say you can never be too careful.

Acknowledgement

This book would not have been possible without the unwavering support of my family, specifically, my lovely wife, Stuti, and my sons. I know I have missed a few important moments over these last several months, but I promise I'll make it up to you soon!

To my mentors in the industry whose work has inspired me to write this book, I owe you a debt of gratitude. To the people who helped me along the way, I owe you a ton of thanks.

To the people who lurked in the shadows and were always ever an email or a phone call away whenever I needed them – thank you for being

available at a moment’s notice! I couldn’t have written this book without you!

Finally, thank you BPB for giving a first-time author this opportunity to write his first book. Thank you for believing in me, in this book, and in the crazy ideas that I kept pitching through the process. You guys are total rockstars!

BASIC (1 point)

Open the Analytics section and toggle all the switches to the OFF position, as displayed in the figure. Note that this screen is likely to look different if you are on a different OS version and if you have an Apple iWatch paired.

Next, open the Advertising section and toggle the Limit Ad Tracking switch to the OFF position. Click the Reset Advertising Identifier … link below that and then Reset Identifier in the confirmation message that appears.

This set of actions ensures that all the previously tracked ads will be dissociated from your account and a new identifier will be assigned to your account, which essentially wipes your ad-tracking slate clean from an advertising perspective.

I strongly recommend that you do this every three to six months to prevent advertisers from building a comprehensive customer profile for you.

Info

Limiting adtracking and resetting the advertising identifier simply means that Apple won't be able to use your usage data to tailor the ads it shows you. Apple will *still* show you ads, only that they are likely to be less relevant.

Preface

“Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively.”

- Wikipedia

Privacy means ensuring that you are able to hide your actions from people who want to snoop on you. Privacy means ensuring that things you do not want to share with the rest of the world do not get shared with the rest of the world. Privacy means being able to choose what others get to know about you. Privacy means having the ability (and the right) to keep certain information -- such as your email credentials, banking credentials, whether or not you like sushi -- completely secret.

Your personal information belongs to you and you alone. It should never ever be available for anyone else to see without your knowledge and without your explicit permission.

Over the last few years, with free/cheap data packs becoming abundantly available more and more Indians have been able to witness the glory of this wonderful innovation called the Internet. Combine them with cheap smartphones, and almost every person on the street seems to be glued to some streaming service or the other.

The Internet, however, is not like any other mode of entertainment - it takes as much as it gives, sometimes more than that. Each time you open an app, each time you click a link, you are conveying a choice, a selection, a conscious effort on your part, and someone somewhere is tracking it all. Every choice your make is being silently recorded. Every page you view is being silently analyzed. Every habit you form is being silently judged.

Moreover, things that you do online are never forgotten; they are remembered for eternity. Anything you post online -- be it a photo, or a video, or audio, etc. -- everything that you share remains on the interwebs forever and ever.

In this book, I argue that privacy is as much a fundamental right as the right to life. In fact, the argument for privacy can be made in the same vein as the example of “The Truman Show” i.e., we need privacy, not because we have something to hide, but because someone else does not get to decide whether or not it is right for us.

This book will help you understand how much of your personal information gets freely shared on the internet without your explicit knowledge and authorization. This book will also give specific and comprehensive instructions on how you can take control of all that information.

By the end of this book, you will have ensured that the information being leaked by your phone, your desktop, your browser, and your internet connection is minimal-to-none. All your online accounts for email, social networks, banking, shopping, etc. will be secure and (significantly) impervious to attackers. You will have complete control over all of your personal information that is available to public view. In fact, if you so choose, you will even be able to create ‘purposeful misinformation’ to counter any potential threats to your privacy and security, if and when necessary.

Over the 15 chapters in this book, you will learn the following:

Chapter 1 introduces a quick self-assessment and establishes some ‘ground-rules’ by defining various terms and concepts such as

#RohitRecommends and the scoring system used throughout this book.

Chapter 2 explains how various devices, services, and adversaries of all kinds have the potential to track and extract your private information by outlining basic and advanced methods to proactively identify leakage of personal information.

Chapter 3 discusses the Android operating system, explores the privacy concerns surrounding them, and provides recommendations on how to deal with such issues.

Chapter 4 looks at the various Apple devices available in the market, attempts to understand the privacy concerns surrounding them and provides recommendations on how to deal with such issues.

Chapter 5 highlights the various issues with the app-ecosystem present in both the mobile platforms – Android and iOS – and provides recommendations on how to identify and deal with such apps.

Chapter 6 explores various 'smart' devices available in the market and how they can impact the privacy of your personal data and provides specific recommendations on how to ensure the privacy of your personal data while using smart devices and/or IoT.

Chapter 7 evaluates how known vulnerabilities in popular desktop operating systems can be exploited by malicious actors to prey on your personal data and provides recommendations on how to deal with these vulnerabilities/exploits.

Chapter 8 evaluates how commonly exploited vulnerabilities in software applications can be exploited by malicious actors to prey on your personal data and provides recommendations on how to deal with these vulnerabilities/exploits.

Chapter 9 evaluates commonly used desktop browsers, discusses how they can be exploited by malicious actors to prey on your personal data, and provides recommendations on how to deal with these vulnerabilities/exploits.

Chapter 10 explores the privacy issues and threats associated with accessing email, how it can be compromised by malicious actors, and provides recommendations to secure your email inbox.

Chapter 11 evaluates different categories of software provided as services (a.k.a. SaaS) over the internet, i.e., Social Networks, Netbanking, Shopping websites, etc. and the privacy issues and threats to consider while accessing these services over the internet.

Chapter 12 discusses the various methods of connecting to different networks (such as Broadband, Wi-Fi, GSM/CDMA, Bluetooth, NFC, etc.) and evaluates each of them from a privacy perspective.

Chapter 13 discusses Operational Security (OPSEC) and presents simple Dos and Don'ts that you can follow to implement OPSEC-like behaviors in your daily routines.

Chapter 14 summarizes all the learning from the previous chapters and invites you to re-assess yourself. If you did everything right up to this point, you should be able to see significant improvement over the results you received in the first chapter!

Chapter 15 contains information that is important to know but a little too detailed for casual reading. You can skip this chapter if you'd like, but I strongly recommend you read it anyway.

INTERMEDIATE (2 points)

If you haven't done it already, I'd strongly recommend that you turn on 2FA (Two Factor Authentication) for your Apple ID. To do this:

Open the Settings app and go to [Your Name]| Password & Security .

Tap on Turn on Two-Factor Authentication and then tap Continue .

Enter and verify a trusted number.

The last step, where you need to enter and verify a trusted number, is a one-time process. Apple sends a verification code that you will need to enter to verify your phone number and turn on 2FA for your Apple iPhone.

There are no further recommendations because this is both the bare minimum that I recommend for everyone and the maximum that Apple provides in terms of pro-active user-input.

Secondly, unlike Google, Apple does not provide a portal to manage your historical data, that is, data that you have shared with Apple until now. Therefore, all data that you have previously shared with Apple remains shared for Apple to use as they deem fit.

Thus, the only thing that you CAN do is to take the proactive steps mentioned above and hope that both Apple's privacy policy and its servers are

secure enough to prevent your data from getting breached.

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors if any, occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Conclusion

Apple devices pose a very interesting conundrum.

On the one hand, they certainly seem to have the more user-friendly options for users to take control of their privacy. However, Apple never fully cedes control to the user.

For instance, all Apple devices come with granular controls to prevent apps from snooping on your data. Apple imposes strict guidelines (read: restrictions) on developers in terms of what data they can and cannot access from the user's iPhone. Apple actively prevents users from installing jailbreaking software.

At the same time, Apple doesn't really allow you to access/modify/delete any historical data. All of your attempts to control your privacy exist only in the moment where you try to control it. Furthermore, a lot of the actions that Apple executes in the name of protecting your privacy , seem to have no associated feedback mechanisms, that is, there is no way to check whether the executed action truly had the intended effect.

In short, while Apple seems to have a robust mechanism for protecting their users' privacy on their device, most of it seems to heavily based on trust rather than transparency.

At the end of the day, all of it boils down to one simple question: Do you really trust Apple to respect your privacy and the privacy of your data? How much?

---

[1] The story goes that Steve Jobs was the one who constantly pushed the Apple engineers to make their products look stylish and sexy, while keeping their essence and operation simple and to the point.

[2] Technically, Apple 'designs' the handset and outsources it to the Chinese manufacturer Hon Hai (English name: Foxconn) who manufactures the actual handset at its factories elsewhere in the world.

[3] SPOILER: The answer is, a rather underwhelming, "Maybe."

[4] As of writing this book, an open-source jailbreaking tool called 'ipwndfu' that could potentially allow jailbreaking millions of iPhones, was being actively researched & developed by an anonymous security researcher called axi0mX.

[5] You can even take a look at what data is being shared from your iPhone under Settings > Privacy > Analytics > Analytics Data, in the entries that begin with Differential Privacy.

Chapter 5

Smartphone Apps

Table of Contents

Section 1: Introduction

1. Prologue

Introduction

Before we begin…

Who should read this book?

How to read this book?

What is #Rohit Recommends?

Basic

Intermediate

Advanced

Expert

The points system

Conclusion

1. Internet and Privacy

Introduction

Privacy? What privacy?!

Google

Microsoft

Facebook

Cambridge Analytica

Adversaries and threats

Passive adversaries

Active adversaries

Intrusive advertising

Invisible threats

What we already know about you

The basics of snooping

Advanced snooping or OSINT

Conclusion

Section 2: Devices

1. Android Devices

Introduction

The Google-Android ecosystem

Android Open-Source Project (AOSP)

So, why does Google do this?

What is a ROM?

Official ROMs

Custom ROMs

Official firmware vs custom ROMs

Android and privacy

Google Telemetry

Non-Google Telemetry

OnePlus Telemetry

Xiaomi Telemetry anddata breach

…and others!

Recommendations and suggestions

Sensors

Permissions

RohitRecommends

Google Telemetry

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

EXPERT: (5 points)

Non-Google Telemetry

BASIC: (1 point)

Sensors

BASIC: (1 point)

Permissions

BASIC: (1 point)

INTERMEDIATE: (2 points)

Conclusion

1. Apple iPhones

Introduction

The Apple Ecosystem

iOS

iCloud

Jailbreaking

Apple and Privacy

Sensors

Permissions

The Settings App

Analytics and Advertising

RohitRecommends

iOS and iCloud

BASIC (1 point)

ADVANCED (3 points)

Sensors

BASIC (1 point)

ADVANCED (3 points)

Permissions

BASIC (1 point)

ADVANCED (3 points)

Settings | Privacy

BASIC (1 point)

Analytics and Advertising

BASIC (1 point)

INTERMEDIATE (2 points)

Conclusion

1. Smartphone Apps

Introduction

Bloatware

How to Identify Bloatware on Android?

Malware

What are the Different Kinds of Malware?

How Do I Know I'm Affected?

Why Doesn't Someone Do Something, Then?

How can I prevent malware attacks in the future?

Sandboxing

Permissions

RohitRecommends

Bloatware

On Android

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

EXPERT: (5 points)

Malware

BASIC: (1 point)

ADVANCED: (3 points)

Sandboxing

BASIC: (1 point)

Permissions

BASIC: (1 points)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

Conclusion

1. Smart Devices and IoT

Introduction

The Internet of Things (IoT)

Security vulnerabilities in IoT and smart devices

Strava

Smart TVs

Alexa, Siri, and Google

Smart appliances

RohitRecommends

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

EXPERT: (5 points)

Conclusion

1. Desktops Operating Systems

Introduction

Operating systems

Microsoft Windows

Modern Windows (Win10, Win 8.1, and Win8)

Windows 7 and older versions

macOS

Linux

Multi-OS systems

Dual boot

Virtual machines

Live OS

Data persistence

Default user: administrator vsguest

Telemetry

Windows 10 telemetry

Diagnostics and feedback

Keystroke logging

Cortana

Wi-Fi Sense

Apple’s Keychain and ‘KeySteal’

Other privacy settings

RohitRecommends

Operating system (OS)

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

EXPERT: (5 points)

Spy vs Spy!

Telemetry

Diagnostics & feedback

Keystroke logging

Cortana

Wi-Fi Sense

Other ‘Privacy’ Settings

BASIC: (1 point)

INTERMEDIATE: (2 points)

macOS

BASIC (1 point)

INTERMEDIATE (2 points)

EXPERT (5 points)

Linux

BASIC (1 point)

ADVANCED (3 points)

Conclusion

1. Desktops-Software Applications

Introduction

Software applications

Bloatware

Manufacturer-branded utilities

Third-party apps and utilities

Integrated Bloatware

Security software

Firewalls

Antivirus and anti-malware

RohitRecommends

Software applications

BASIC (1 point)

INTERMEDIATE (2 points)

ADVANCED (3 points)

Sandboxing

File encryption

System restore

Bloatware removal

Windows 10

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED (3 points)

EXPERT (5 points)

Apple (macOS)

BASIC: (1 point)

Linux

BASIC: (1 point)

Security software

Windows 10

Firewalls

BASIC: (1 point)

INTERMEDIATE: (2 points)

Antivirus & Anti-malware

BASIC: (1 point)

INTERMEDIATE: (2 points)

macOSand Linux

BASIC: (1 point)

Antivirus andanti-malware

ADVANCED (3 points)

Antivirus and anti-malware

Conclusion

1. Desktops-Browsers

Introduction

How do modern browsers work?

Popular browsers

Privacy-aware browsers

Brave browser

Epic browser

The Tor browser

Is Tor truly anonymous?

Privacy settings

Private windows

Telemetry opt-out

Syncing and personalization

Search engine integration

Cookies, tracking, and content blocking

Forms and autofill

Permissions andsite settings

Plugins and extensions

The difference

Plugins and extensions are fundamentally different

Potential security concerns with plugins

Potential security concerns with extensions

RohitRecommends

BASIC (5 points)

Browser recommendation

Private browsing

Privacy settings

Extensions

INTERMEDIATE: (10 points)

ADVANCED: (15 points)

Browser recommendation

Private browsing

Privacy settings

Extensions

EXPERT: (25 points)

Installing Tor

Using Tor

Caveat Emp-tor!

Conclusion

1. Services - Email

Introduction

Email

Accessing email

Web-based portals

Email clients

Compromising your email

Phishing

Weak passwords

Malware

Email ads

Hosting your own email server

Using a privacy-aware email service provider

Spam

RohitRecommends

Accessing your email

Web-based portals (BASIC, 1 point)

Offline clients (BASIC, 1 point)

Introduction

Compromising your email

According to data made available by AppAnnie , in 2018, consumers downloaded 194 billion apps in total, spent $101 billion (up 75% from 2016) in apps stores, and averaged three hours a day on their mobile phones. That's more than the money people spend on music (live AND recorded), twice the amount of money people spend on sneakers, and three time the size of the oral care industry! It is estimated that app store consumer spend will surpass $120 billion in 2019—double the size of the global box office market!

Phishing

According to data made available by AppBrain , as of February 2019, the total number of iOS apps available was around 2.2 million. Google Play store reportedly had over 2.7 million apps as of July 15th 2019. Of these, a little over 57% of apps use an ad network.

BASIC: (1 point)

On average, smartphone users have about 80-90 apps installed on their phone and launch an average of between 5 and 9 apps a day, and more than 30 apps on a monthly basis. This trend, surprisingly, has remained consistent since 2015 and is now known as the 30:10 rule, that is, 30 apps a month, 10 apps a day.

Passwords and authentication

BASIC: (1 point)

Malware

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

Email ads

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

EXPERT: (5 points)

Spam

BASIC: (1 point)

INTERMEDIATE: (2 points)

ADVANCED: (3 points)

EXPERT: (5 points)

Prevention and mitigation

BASIC: (1 point)

INTERMEDIATE: (2 points)

Conclusion

1. Software-as-a-Service (SaaS)

Introduction

So, what exactly is SaaS?

Types of SaaS

Social SaaS

Shopping SaaS

Financial SaaS

Other SaaS

Privacy and security concerns

ToS and privacy policy

Service reliability

Security and transparency

Security breaches and response

Security updates

Data access

RohitRecommends

Types of SaaS

BASIC (1 point)

INTERMEDIATE: (2 points)

ADVANCED (3 points)

EXPERT (5 points)

SaaS privacy concerns

ToS and privacy policy (BASIC, 1 point)

Service reliability (ADVANCED, 3 points)

Security and transparency (EXPERT, 5 points)

Security breaches and response (INTERMEDIATE, 2 points)

Security updates (EXPERT, 5 points)

Data access (ADVANCED, 3 points)

Conclusion

1. Networks: Connectivity and Internet

Introduction

Wired networks

Wireless networks

Wi-Fi/WLANs

GSM

Bluetooth

NFC

Common attack vectors

Identification

Interception

Wireless attack vectors

Bluetooth

NFC

RohitRecommends

BASIC: (1 point)

INTERMEDIATE: (2 points.)

ADVANCED: (3 points.)

EXPERT: (5 points)

Conclusion

1. Operational Security (OPSEC)

Introduction

An adversarial approach

The OPSEC process

Dos and Dont’s

Mobile phone subscription

Device security

New signups

Conclusion

1. Epilogue

Introduction

Updated analysis

Conclusion

1. Bonus Chapter: Useful Tips and Tricks

The 10 Android permissions listed under “dangerous” protection level.

How to setup your Android without Google Services

Useful apps that you should definitely consider installing

Alternative app stores

For Android

For Apple

Conclusion

Checking your email on an unknown computer

Bloatware

When you switched on your smartphone for the first time, you probably saw a bunch of apps that are not a part of the official operating system, i.e., apps that are not critical for the operating system to function. Some of these apps may even be really popular apps, for example, Xiaomi bundles the Facebook app with MIUI on most of its phones. Apple bundles the Stocks app on iPhones.

For the purposes of this book, I will be defining bloatware as an app that is not a part of the core operating system or actively installed by the user, regardless of its popularity. In some cases, users don't even have the option to remove the app– only disable them! Most users neglect them and they continue to remain on the phone, hogging valuable system resources.

Section 1

Introduction

How to Identify Bloatware on Android?

Typically, apps on a smartphone can be broadly divided into two categories – (pre-installed) system apps and downloaded apps.

Say, you have a hundred apps installed on your phone, including the apps that were already installed when you bought the phone. Let's try and isolate the different categories of apps that you are likely to use, shall we?

Hourly usage: Email, browser, messaging (for example, WhatsApp, Signal, Facebook messenger, Telegram, and more).

Daily usage: Games, social networking (for example, Facebook, Twitter, Instagram, Snapchat, and more).

Weekly/monthly usage: Payments, banking, and more.

Random usage: Productivity, tools (for example, calculator, the camera, the clock, contacts, and more); settings; maps; shopping; entertainment (for example, Netflix, Amazon Prime Video, Saavn, Gaana, Spotify, and more).

Hopefully, you were scrolling through your apps while reading the bullet points above. Did you notice any app on your phone that did NOT get accounted for in the previous paragraph? Those are the apps that you need to look at and ask the following questions:

Do I need this app at all?

If I don't need it, can I remove it?

If I can't remove it, what exactly is it doing on my phone?

If you answered, "Uh, I downloaded that app when I was bored and looking for something but I forgot to uninstall it," then now would be a good time to uninstall that app.

If you answered, "Android won't let me uninstall this app because it is a 'system' app," then it is likely to be pre-installed bloatware that you don't need.

In either case, chances are that the app is probably collecting information and sending it somewhere.

Chapter 1

Prologue

Malware

While bloatware refers to apps that come pre-installed on your phone, malware (short for malicious software) refers to those apps that are primarily designed with the intent of stealing or damaging your device and data.

Introduction

Hello, there! Before you dive into the rest of this book, I'd like to ask you to do something.

Take your smartphone, open the scanner app (or the camera app, if it supports QR code scanning) and scan the QR code that is printed on this page.

What are the Different Kinds of Malware?

The most common types of malware that can affect your device are viruses, Trojans, spyware, ransomware, and many more.

Viruses are malicious programs that replicate by attaching to another program. However, most modern phones such as Android and iPhone cannot

technically have viruses because each application on Android runs within its own 'sandbox', that is, it cannot exchange any data with other apps unless explicitly given permissions (or privileges) to do so.

Spyware and Trojans are the most common forms of malware that affect Android users. Malware of both these kinds usually install hidden services that are able to collect and send your personal data to thirdparties without your consent.

Ransomware is a kind of an application that locks the user out of the device, that is, holds them ransom. In some cases, it may take over your device and encrypt it further. The users will remain locked out until a payment is made to some anonymous cryptocurrency account, after which a decrypting mechanism/key may be provided to unlock the device.

Info

The Android PNG Malware Exploit

For a long time, it was believed that you could not get malware on your phone unless you actively made a choice to install it. However, all that changed early this year (February 2019) when Google disclosed in its security update that there was a flaw that could allow a malicious actor to install malware on a target phone by simply sending a PNG image.

That means your phone could be infected with malware just because you innocently tried to open a malicious image. The situation becomes even worse when you think of the many ways in which this can happen accidentally.

Although Google fixed the vulnerability in February itself, the fix has not been pushed to all Android devices. If you want to check whether your phone is up-to-date and protected against this vulnerability, you can do so by following these steps:

Open your Settings app.

Scroll down to the bottom and open the About Phone section.

Check the Android version, specifically the date mentioned under the subsection titled Security Patch .

If the date happens to be a date *after* February 2019, you can consider yourself protected from this vulnerability. If not, consider upgrading either your operating system or your phone, at the earliest.

Open the link that is presented to you on your screen and follow the instructions on the page.

Alternatively, open the browser app on your phone and visit the following webpage:

https://leaktest.privacy.clinic

Now, you must have received a short alphanumeric code from the website. Note it down here:

This alphanumeric code will come in handy in future chapters. Note it here before you forget it!

When you are done, turn the page, and start your journey!

How Do I Know I'm Affected?

A malware infection on your device can be likened to your device being ill —you will immediately know that something is not right.

Your device may suddenly start acting sluggish, freeze occasionally, or throw up some junk on your screen. Or you may find the browser displaying random websites with suspicious-looking URLs in the address bar. Ads may pop up at random times and you may find yourself being subscribed to random paid services without your knowledge and/or intervention.

Info

Malware is NO Child's Play!

A white-paper by Rubica published in February claims that kids are a lucrative target for cybercriminals. One, their lack of knowledge combined with a casual attitude makes then vulnerable to clicking random ads, which might install malware-by-proxy. Two, their behaviors can be manipulated by cybercriminals to acquire wider and/or deeper access to their parents' data—since most parents often share their devices with their kids.

In fact, the Rubica whitepaper found that some of the most popular kids' games often displayed aggressive interaction behaviors, such as excessive ads, unsafe download prompts, invasive permissions that grant access to device logs, history, location, microphone, etc. This set of behaviors shares multiple similarities with the behaviors of cybercriminals trying to access personal data of targeted users. Popular games such as Fruit Ninja, Talking Tom, Angry Birds, and more, were evaluated and found to be unsafe enough to require parental supervision and intervention from time-to-time.

Scan the QR code given alongside, in this info box, to read the entire white paper on the Rubica website.

Before we begin…

We -- as in, you and me -- are going to make a few assumptions about what it means to ensure the security and privacy of your data by enumerating the following rules of data-sharing:

If the data is not encrypted and not in your control, then it is neither secure nor private. Storing your data unencrypted on remote servers is like keeping your data in an open book. Finding ways to access this data is the very definition of what hackers do day in and day out. For example, most of the leaks catalogued by services like HIBP (Have I Been Pwned), dehashed, and more.

If the data is in your control, but you can’t encrypt it, then it might be private but it is not secure. A person with physical (or even digital) access to your data can still access it without your knowledge or permission. For example, plain-text passwords stored in browsers, or worse, in an Excel file on someone’s PC!

If the data is encrypted, but not in your control, then it might be secure but it is not private. No matter how well it is encrypted, assume that an adversary already has access to it or might eventually have access to it. The toughest encryptions can (and will) be eventually broken, leaving you exposed to all kinds of potential attacks. For example, data stored on remote servers.

Only when your data is encrypted and in your control is when we can assume that your data is completely secure and private.

Two things to note:

You can never achieve 100% security and privacy of your data. The field of information security and privacy is always changing, with new vulnerabilities being discovered and new exploits being revealed every single day.

You can achieve close to 100% security and privacy of your data if you really want. However, this will require a LOT of technical know-how and expertise. You will also have to make many, MANY sacrifices along the way.

Don’t get me wrong, I am NOT saying that security and privacy on the internet is an impossible goal! On the contrary, I’m saying that you do not have to trade ALL of your comfort for the privacy and security of your data!

The comfortability of data-sharing is a broad spectrum. It ranges all the way from people who are comfortable sharing all kinds of data with any third parties, to people who are uncomfortable sharing any kinds of data with all third parties. You can trade none of it or trade it all away, if you want – the choice is entirely up to you!

[QR Code: https://rubica.com/wp-content/uploads/2019/02/Rubica-Report-Cyber-Crime-Privacy-Risks-in-Free-Mobile-Kids-Apps.pdf]

Who should read this book?

Everyone. Regardless of whether you are simply curious about privacy as a concept or have just begun your journey into securing your digital

footprint, or you are a veteran of masking your presence online, this book will help you achieve the level of digital invisibility that you'll feel comfortable with.

I've attempted to keep this book as conversational as possible. While subsequent chapters will enumerate the potential risks associated with various devices, services, and many more, I will also enumerate ways to remove, reduce, or mitigate these risks.

Our endeavor throughout this book has been to provide insight into how your data is being shared with third parties—often without your consent—and what you can do to mitigate or, failing that, obfuscate it.

Why Doesn't Someone Do Something, Then?

In 2012, Google introduced a service codenamed Bouncer that provides automated scanning of apps submitted to the Play Store before making them available for download. Google Bouncer analyzes apps for any signs of hidden, malicious behavior and prevents suspicious apps from appearing on the market.

Info

Google Bouncer isn't a perfect service and some malware might still make it through the cracks. For example, in August 2019, an app called Radio Balouch found its way onto the Google Play Store, despite the fact that it contained the open-source spyware called AhMyth. Similarly, researchers from Kaspersky Lab revealed that the popular app CamScanner was also carrying malware, prompting immediate removal from the Google Play Store.

This doesn't mean that Google Bouncer doesn't work; it only means that no system is perfect and some malicious apps might still manage to slip through the cracks.

Apple has a separate team that analyzes each and every app that goes on to the Apple iTunes store. All apps in the official Apple ecosystem are thoroughly tested and vetted before being released to the general public.

Note that both Android users with rooted devices or Apple users with jailbroken devices are considered to be under tremendous risk of malware infection. Such users are probably likely to install apps from random unknown sources, which may further increase the severity of a malware infection.

How to read this book?

I've tried creating this book as an interactive piece to work with. That means, at times, I will provide a QR code alongside the content. The QR code is meant for you to scan and read, watch, or do something on the internet and then return to the book. Think of these as the book-equivalent of hyperlinks that are meant to guide you to additional resources on the topic.

This book is meant to be a textbook and a workbook both—I highly recommend keeping your devices nearby while reading this book. As you progress through this book, you may identify some scenarios are directly applicable to you, while others may be irrelevant.

I will be providing you with various recommendations pertinent to the subject matter that is being discussed. Consider each recommendation carefully and choose whichever recommendation suits you best, that is, perform the tasks as instructed, immediately, on your phone, tablet, laptop, or online. Not every recommendation might apply to your specific scenario but some (or maybe, most) things will definitely apply. Choosing NOT to act on them would be a very bad idea.

I've also included a scoring system in the book to help you monitor your progress, as you read. This scoring system is based on the expertise and effort required to follow the aforementioned recommendations. You'll find these recommendations neatly tucked under a separate heading called #RohitRecommends.

How can I prevent malware attacks in the future?

The easiest way to prevent malware attacks is to install a good antivirus/antimalware app that will do the job for you, but we strongly recommend that you also comprehensively review your browsing habits.

Are you the kind of person who believes that you are actually the millionth visitor to a website? Are you the kind of person who thinks random websites legitimately give away expensive gadgets for cheap, or even free? Are you the kind of person who gladly shares their contact details with all websites that ask for it? If you answered yes to any of these questions, then your troubles go way beyond the scope of this book. You desperately need what is called "Basic Awareness while Browsing the Internet."

For those of you in a hurry, here's the short version of it:

If it makes you think Wow! I am so lucky! or Did I participate in that? or something along those lines, it is almost definitely a scam. Do NOT fall for it.

As a rule of thumb, do NOT share your mobile number or your email address with anyone. If you absolutely must, maintain a separate number and email address to give out in such situations.

If the application being installed is named differently from what you clicked, or requires elevated, administrator privileges, or requires you to install something unrelated first, ABORT the installation right away.

The cardinal rule to prevent malware infections (which is also applicable to browsing the internet, in general) can be boiled down to three simple words:

"TRUST, BUT VERIFY."

What is #Rohit Recommends?

At the end of each chapter, I have presented several recommendations categorized neatly into four categories: Basic, Intermediate, Advanced, and Expert.

The recommendations under each of these levels are (mostly) progressive, that is, you'll (probably) have to fulfill the recommendations under the Basic level, before following the Intermediate recommendations. Each recommendation level is assigned a score, based on the amount of effort required to perform the tasks mentioned in the recommendation. In some cases, you might find only a single level of recommendation—that's probably because there isn't much else to recommend in that context!

Basic

Sandboxing

When you install an app on your Android device, it is copied to the system partition (a.k.a. internal storage) and allocated a folder that can be accessed only by the app. However, the app may choose to store some data on the external storage, which is the partition accessible to everyone —user, as well as other apps.

The problem is, the Android external storage isn't sandboxed, that is, apps that have been granted permissions to read and write to external storage can read any and every file on your external storage. What this means is data can be freely shared between different apps when it is stored on the external storage of your device.

That means, if you happen to download sensitive information, such as your bank statement from your banking app and store it in the Downloads folder in your external storage, any app with access to that folder can access and read that file without your explicit permission.

Info

External storage typically used to refer to removable storage in previous Android versions, but in recent versions, it has taken on the rather vague meaning of that partition of phone storage, which is accessible to apps for storing and retrieving information that can be copied to and from the phone to other external devices such as USB, PC, and more. Typically, this is also referred to as the 'data' partition on your phone.

Who: This level is intended for people who are curious about the privacy and/or security of their data and would like to have a clearer picture of how sharing (or not sharing) of this data might affect their digital experiences.

What: At this level, we will primarily gather information that will help you understand the security and/or privacy issues associated with the subject under consideration. In some cases, I may even recommend a few simple actions that you can take (almost) immediately, without significantly hindering your usage habits or your overall digital experience.

Example: If you are a heavy Facebook user who needs to continue using Facebook, I would recommend opening your Facebook settings and clicking on each option in the side bar, one-by-one, and turning off all the options that result in oversharing of your data.

Intermediate

Permissions

In its early days, Android adopted a very relaxed permissions model , that is, apps were allowed to ask for any permission from the user. This led to

a bunch of apps misusing and abusing the liberal permissions model [1] , until Google was forced to crack down on such unethical behavior.

Until Android v6.0 Marshmallow, these permissions were granted to the apps at the time of installation. However, starting from Android v6.0 Marshmallow, runtime permissions were introduced, which allowed users the ability to grant or deny permissions when the app was actually being used. Runtime simply means that the app needs to ask for permission when it is 'run' by the user, and not just at the time of installation.

Moreover, the internet permission is no longer classified as a dangerous permission since Android v6.0 Marshmallow, that is, all apps are now allowed to use your device's internet connection, if they wish to do so. This means, an app with a set of rogue permissions can collect data and share it silently with third-parties without your explicit permission to do so. For example, a malicious app with READ/WRITE EXTERNAL STORAGE permission can silently upload all files stored on your external storage to a remote server without your knowledge. If your bank statement happens to be in the Downloads folder, well, bad luck!

Additionally, apps do NOT need to be given all the permissions that they ask for. You are free to grant certain permissions, and deny other permissions to the app. If the app is well-designed and well-developed, it can handle this loss of permission properly, without crashing. If the app does crash, then it is probably a sign that you might want to look for an alternative.

Why deny permissions, you ask? Well, because most apps will try and collect as much data about you, as they can. For example, the Google app requests the location permission to ensure that it can relay back accurate location information to Google servers for the Find My Phone feature. However, granting the location permission to the Google app means that it can be used by the Google app to provide you location-relevant search results.

Info

You can't run and you can't hide…

Even if you deny location permissions to the Google app, it will still try and narrow your location based on the IP address, recent locations, or Location History. In some cases, Google has been known to utilize telemetry data, such as Wi-Fi and cellular network information, to serve you location-aware results when you search on the app. Don't believe me? Try searching for "Chinese Restaurants" on your Google Search app.

Notice how Google immediately tries to identify your location and provides you location-aware results at the very top.

Now, some of you may argue that it is a trade-off for being able to know where your phone is all the time. However, it leaves the door open for multiple malicious actors to leverage this through nefarious means.

Who: This level is meant for people who are concerned about their data being shared without their active consent and want to take steps to mitigate it—provided it doesn’t interfere with their daily experiences with digital devices.

What: At this level, we will utilize the information gained in the Basic level AND provide you with options that will help stem the leakage of your personal data. At times, I might even recommend tweaking a few system settings, a little bit. A rudimentary knowledge of computers and a superficial understanding of how the internet works would be considered an added bonus at this level.

Example: To continue the previous example, I’d recommend using a third-party app to access the Facebook service—preferably one that is more privacy-aware than the default app such as Simple Pro or Phoenix. We’d also recommend installing an ad-blocker on your device (that is, smartphone or computer) to further reduce giving away your details to unsecured third parties.

RohitRecommends

When it comes to smartphone apps, I believe in the motto Less is more.

The fewer apps you have on your smartphone, the lesser the chances of your information being leaked to various third-parties. It also reduces the available attack surface for adversaries. However, this is not easy to achieve, given that we live in a world in which the number of apps and the number of malicious actors keep growing, every minute of every day.

Advanced

Bloatware

Here are a few methods to quickly and cleanly identify (and possibly get rid of) unnecessary bloatware on your smartphones and tablets.

Who: This level is meant for people who guard their privacy fiercely and would like greater control over their data. It requires a broader understanding about computers, (maybe) some bit of programming, and a more-than-superficial understanding of how the internet works.

What: At this level, we might require you to put your security and privacy concerns before everything else. A willingness to change long-standing habits and the ability to adapt to new situations and experiences will be very useful at this level.

Example: To continue the Facebook example, we recommend deleting the native Facebook app altogether and recommend that you use a privacy-aware browser—both on the desktop or mobile—for all of your Facebooking needs.

On Android

(Overheard somewhere…)

Q: How do you get rid of bloatware on Android?

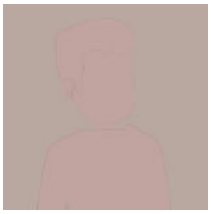
A: With great difficulty…

Jokes aside, since bloatware is directly influenced by the phone manufacturers, they have very little incentive to provide proper uninstallation methods. Often, you'll find that there is no uninstall option for these apps—you can only Force Stop them or Disable them, or in some cases, Uninstall Updates . None of these options removes the apps completely from your system.

BASIC: (1 point)

Open the Settings app on your phone and scroll down to the Apps section. Click on it to open it and select the option that allows you to view all the apps on your system. One-by-one, click on each app and ask yourself the question, "Do I really *need* this app? Or can I do without it? Can I access the same functionality using a browser?" If the answer is not an emphatic, "I NEED THIS APP!", then the app doesn't need to be on your phone and can probably go:

Expert



Who: This level is aimed at a very specific subset of people in society – people for whom maintaining privacy is a necessity, rather than a curiosity. Celebrities, law enforcement officers, soldiers, people enlisted in sensitive jobs such as the defense sector (that is, the army, navy, air-force, and many more) or people working in various intelligence services might want to consider this level.

What: At this level, you are expected to have significant knowledge of the subject matter under consideration and deep knowledge of the alternatives. I strongly recommend acquiring the services of a trusted person who can assist you with the same. A deep knowledge of computer systems, software programming (primarily working with APIs, web applications, and such), and a very good understanding of how the internet works is highly recommended.

Example: To continue the running example, we'd recommend that you stop using Facebook in its entirety. Instead, we would suggest that you utilize alternative methods of communication to reach out to your Facebook audience.

I strongly recommend that you consult with an expert (or experts) before attempting any of the Expert recommendations presented anywhere in this book. I shall not be held liable for any loss of any kind if anything goes against expectations or yields a less than desirable outcome, for those who insist on following any Expert recommendations without proper supervision or consultation.

Info

Advanced vs. Expert –What should YOU choose?

Many people recommend deleting your Facebook account entirely to ensure that Facebook cannot collect any data on you. However, this is somewhat misleading and, in some cases, against common sense.

For example, as a cyber-security expert, I need to use Facebook for two primary reasons: to promote myself and the various services I offer and for personal purposes.

However, I have taken great care to ensure that those two parts of my life (that is, personal and professional) are kept strictly separate on Facebook. There are various steps one can take to achieve a proper balance between being connected and staying private on Facebook. We'll be discussing all of these steps (and a lot more) throughout this book.

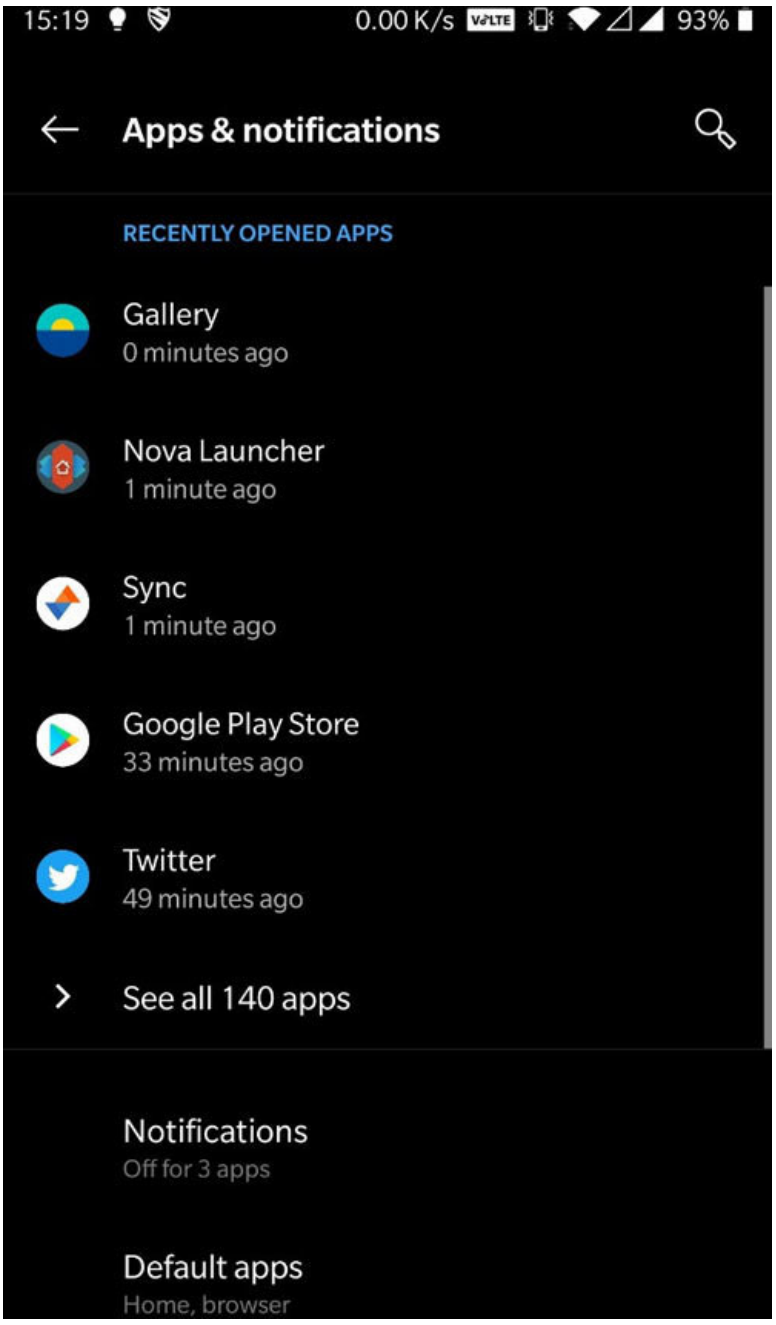


Figure 5.1: The 'Apps & notifications' section in the "Settings" app as seen on a OnePlus 5, running OxygenOS version 9.0.9

For example, the shopping apps you have installed on your phone get used only once in a blue moon. However, you can be sure that they are constantly sending data on your phone usage habits and analyzing your usage patterns.

The points system

You already know about the four recommendation levels viz. Basic, Intermediate, Advanced, and Expert . You can choose to follow the recommendation that makes the most sense to you, and it doesn't have to be the same level in every case.

For instance, you can choose to follow the Advanced recommendations in the Chapter 9: Browsers , but only the Basic recommendation in the Chapter 10: Email .

Each recommendation is assigned a specific point score. In most cases across the book, a Basic recommendation is worth one point, Intermediate is worth two points, Advanced is worth three points, and Expert is worth five points.

Remember, you do not have to follow ALL the recommendations, only ONE of them!

Note

In some cases, you might find that the recommendations are progressive, that is, the previous level must usually be completed before proceeding to the next one. However, you DON'T have to follow them ALL the way. If you feel that the ADVANCED level is too technical or prohibitive, you may stop at the INTERMEDIATE level itself. You will then earn points for BASIC and INTERMEDIATE both, but not for ADVANCED or EXPERT.

You can keep a scoresheet of sorts by entering the points you 'earn' in any of the following places:

The Table of Contents

The Scoresheet at the END of the book

Print out of the softcopy of scorecard available on the website

After you finish reading/working through the book, tally up your points and see your progress. This will help you to get re-motivated to take more steps forward to further protect the privacy of your personal data.

Additionally, this book is designed in such a way that the information being shared by your phone/device changes with each recommendation you follow in the course of reading this book. You can track it for yourself, if you want.

Scan the QR code given alongside this paragraph or open the following link in your browser:

INTERMEDIATE: (2 points)

Once you have identified the bloatware app you want to remove, you can either uninstall the app or disable it.

Uninstall: To uninstall an app, long press the app icon either in the app drawer or on the home screen, then click on (or drag the app to) the trash can icon to uninstall it. Alternatively, you can go to Settings | Manage Apps and scroll down to the app, tap on its name, and then click on Uninstall .

Disable: Some apps (such as the apps provided by Google Mobile Services) only allow you to disable them rather than uninstall. Clicking Disable is somewhat similar to uninstalling, except the app isn't completely removed from your phone—you can re-enable the app at a later date, if you wish.

Google provides detailed instructions on how to 'disable' system apps. Scan the QR code given alongside this section to open the official Google Support page that details this procedure.

https://book1.privacy.clinic/scorecard

You'll need to enter the alphanumeric code (the one that you hopefully did note down at the beginning of the chapter) to access your privacy leak-test score. If you didn't note it down, don't worry – just go back to beginning of the chapter, scan the QR code, visit the webpage again, and generate a fresh code; and, this time, don't forget to note it down in the empty box provided on the first page!

[QR code: https://support.google.com/googleplay/answer/2521768?hl=en]

Conclusion

A lot of people around me keep asking me what they can do to protect their privacy on the internet. Let me just put it this way. If there were a simple answer to this question, I would have simply tweeted it out instead of writing a whole book about it!

Don’t worry though, it isn’t as difficult as some of the articles want you to believe. Some of it involves some intricate steps but nothing that you can’t do by yourself. In fact, that’s the whole purpose of this book—to get you to question everything and take nothing at face value.

The ONLY thing I ask of you is this: Don’t just read this book. Work with it, with me.

I’ve even tried to gamify this book by assigning points to various actions so that there is sufficient incentive for you to follow my recommendations. You may not like the points system, but believe me when I say that it works like a charm. Keep telling yourself that your target for this book is to score as many points as possible in the next 12 chapters. You don’t have to score the maximum every time. Just like a cricket match, score singles and twos here-n-there and hit the occasional full-toss over the ropes!

If you do, I can assure you that it will help you gain control over your data, your privacy, which is supposed to be YOUR choice.

ADVANCED: (3 points)

Important!!

The actions described in this section require your Android phone to be rooted. If you have NOT rooted your device, do NOT read any further—skip this section and head straight to the next one!

A quick search of the keyword bloatware on the Google Play Store reveals that there are many apps that will help you uninstall bloatware from your rooted device—many of them made by reputed companies and developers.

However, the best app and the one that many, many experts on the internet will recommend without hesitation is Titanium Backup Pro. You'll need the full version with the Pro license to use its best features. It costs 400 INR (as of September 2019) on the Google Play Store, but it is worth every rupee.

Important!!

NEVER EVER MAKE ANY CHANGES TO YOUR PHONE WITHOUT CREATING A FULL BACKUP FIRST!

Install Titanium Backup Free, and then install the companion license app, i.e., the Pro key. Launch it and grant it superuser permissions when it prompts you.

You can now decide whether you want to Backup, Freeze, or Uninstall the offending bloatware apps. To do this, you need to open the Backup/Restore tab, scroll down, and tap on the name of the app. A dialog box opens with details about previous backups and displays the three actions: Backup, Freeze , and Uninstall .

1) Use the Backup button first to create a backup of the app, in case something goes wrong.

2) If you want the app to still be available in case you change your mind, tap the Freeze button at the top.

3) If you are sure you want the app to absolutely disappear, tap the Uninstall button instead.

Frozen apps can be defrosted in Titanium Backup Pro by repeating the same steps as above, and clicking Defrost instead of Freeze . Uninstalled applications need to be re-installed or can be recovered.

Alternatively, on rooted phones, you can also use a regular root-aware file manager app, such as Root File Explorer Pro, to carry out bulk deletions of bloatware apps. Be careful, though, you are very likely to break apps if you don't know what you are doing.

Chapter 2

Internet and Privacy

EXPERT: (5 points)

Important!!

The actions described in this section require your Android phone to be rooted. If you have NOT rooted your device, do NOT read any further—skip this section and head straight to the next one!

Buckle up, because this involves connecting your phone to the PC and making changes to it using the Android Debug Bridge (ADB). A detailed guide can be found on XDA forums here:

Introduction

Imagine you were rich – like, pre-divorce Jeff Bezos' kinda rich.

Imagine that you decided to hire a personal assistant, like a butler. Except, this butler would take care of everything for you, up to the point where all that remains to do is making a yes-or-no decision. What's more, your butler also notes down your preferences and updates their suggestions accordingly the next time. Your morning would end up looking something like this:

Your butler comes in to wake you up at 6 AM. You could wake up ("Yes.") or you could refuse to wake up ("No…").

Butler's Notes: "0600: Did not wake up."

He comes back five/ten/fifteen minutes later and repeats the question until you decide it is time to wake up.

Butler's Notes: "0605: Did not wake up"

Butler's Notes: "0610: Did not wake up but seems partly awake."

Butler's Notes: "0612: Woke up. Number of wake-ups required: TWO. Time between first wake-up call and actual wake-up: 12 minutes"

He then offers you the morning newspaper along with tea and breakfast in bed. You could accept it ("Yes.") or refuse it ("No…").

Butler's Notes: "0615: Accepted tea. Refused breakfast-in-bed."

Then you go shower and start getting ready for the day.

Butler's Notes: "0629: Went to shower."

Your butler now presents you with your clothes. You reject his first suggestion of a black shirt ("NO."), reject his second suggestion of a purple shirt ("No…"), and accept his suggestion of a pink shirt ("Yes.").

Butler's Notes: "0645: Came out of shower. TOTAL SHOWER TIME: 16 minutes"

Butler's Notes: "0646: Rejected BLACK shirt."

Butler's Notes: "0647: Tried PURPLE shirt. Rejected."

Butler's Notes: "0648: Chose PINK shirt. TIME TO CHOOSE: 2 minutes"

You get the general idea, right?

Over time, your butler builds up a pretty accurate idea of your choices and preferences. He is able to make suggestions that are so perfect that you simply can't refuse! It's like he knows you inside and out! He is the Jeeves to your Bertie Wooster, and you absolutely couldn't live without him. In fact, you have come to trust him so blindly that you don't bother reviewing your options and just end up accepting the first option he presents to you. Hey, it saves you time and your butler just seems to know what you like, doesn't he?

Except this butler isn't Jeeves and lacks one crucial quality – loyalty.

While you were blindly trusting him with some of the most intimate details of your life, your butler was selling those notes he was making about you to the highest bidder. You've heard whispers of it happening but it doesn't bother you. After all, what difference does it make if he tells people what color shirt you prefer to wear, right?

Turns out that the information collected by your butler was used by your grocer to sell you a more expensive tea. It was used by your designer to dress you up in darker shades. It was used by your newspaper agent to sell you a subscription to a brand of journalism that espouses slightly more

left-leaning (or right-leaning, depending on your preference) point of view.

So, although you didn't notice it at first, things have certainly changed since he took over your life. Your brand of tea is different, you wear darker shirts more often, and you no longer read The Expressive Indian; you now read the The Times of Timbuktu instead!

By now, you must have latched on to the fact that this hypothetical example isn't entirely hypothetical.

The butler in question could be your smartphone. Or your smart TV or your smart refrigerator or your fitness tracker. Any internet-connected device, really.

Because that's exactly what they are meant to do. Gather data, and build your profile. A profile that can be used by various advertising networks to show you ads on the various sites you visit on the internet, like Google, Facebook, Twitter, Instagram, to name a few.

[QR Code: https://www.xda-developers.com/disable-system-app-bloatware-android/]

To sum it up quickly, here's what you'll be doing:

Install the ADB drivers, download the Android SDK platform tools and unzip them to a convenient directory of your choice, and connect your phone to the PC.

Use an app like App Inspector or drill down in App Info to figure out the package name of the bloatware app that you want to remove from your phone. For example, the package name for the Google Chrome browser is com.android.chrome

Open a Command Prompt or PowerShell window (or a Terminal window, if you are a Mac user) in the directory with the ADB binary and enter the following command depending on your OS:

Windows Command Prompt:

adb shell pm disable-user --user 0

Windows PowerShell:

.\adb shell pm disable-user --user 0

Mac/Linux Terminal [2] :

./adb shell pm disable-user --user 0

Note

There are various apps available on the Google Play Store that claim to disable/uninstall all kinds of bloatware and malware, even on unrooted phones. While a few of them may actually perform as advertised, most of them are themselves suspect. I strongly recommend that you consult with someone who is knowledgeable about Android phones before you install any such apps!

Removing Bloatware on Apple Devices

Getting rid of bloatware on Apple iPhones is a three-step process:

Switch on your iPhone.

Press and hold the app that you want to remove or delete—hold till all the apps on the screen start shaking.

Tap on the red x button to delete the app.

That's it, you're done!

Privacy? What privacy?!

A 2018 report published jointly by IAMAI and Kantar-IMRB estimated the number of mobile internet users to be around 500 million. Judging by the

growth pattern in recent years, we could say that the number of mobile internet users is rapidly approaching a 1:1 ratio, that is, every adult carries a device capable of connecting to the mobile internet.

Did you know, the technology that exists today allows each one of those 500 million users to be uniquely identified?

Malware

In the event that your phone is infected with malware, you should take immediate steps to identify and remove it from your system.

Google

When you sign into a Google account on your smartphone, Google generates a unique identifier for your phone called the Google Advertising ID. You can verify this yourself. If you have an Android phone, open your Settings | Google , then under Services , click on Ads . You'll see the advertising ID assigned to you by Google at the bottom; it'll look something like this:

Your advertising ID:

x12xxxx3-456x-7xx8-xx90-xx1xx2345x6x

Hint

You can opt-out of Google's Ad personalization by toggling the switch that you see here, that is, you'll still be shown Google's text ads on various sites but Google will not associate your browsing behavior and your usage across various Google accounts to personalize these ads in any way.

Everything you do on your Android phone is being relayed to Google's servers, and their algorithms are crunching all the data to figure out what your likes and dislikes are and how best to serve you content and ads that are tailored to your likes and dislikes.

It's not just Google, by the way.

BASIC: (1 point)

Uninstalling suspicious apps: Open your Settings app and navigate to the list of Installed Apps . See if you can identify any apps that you did not (consciously) choose to install and remove them immediately. If you are not sure about an app that is installed on your device, search for relevant details on the internet.

Third-party tools: You can also use one of the many antivirus/antimalware apps available in the Play Store. Some of the more popular ones are Security Master, Bitdefender, AVG, Malwarebytes, Quick Heal – again, the internet is a rich source of information for choosing the right one for your device.

Microsoft

In the summer of 2015, Microsoft released Windows 10 and offered it as a free upgrade to all Windows 7 users – genuine and otherwise. Many users took them up on the offer without realizing that Windows 10 sends a lot of telemetry information back to Microsoft servers by default. Even if you choose the option to NOT share any information, Microsoft collects what it calls Basic diagnostic information.

Have you ever wondered what is included in Basic diagnostic information? Well, Microsoft has been kind enough to tell us themselves!

"Basic: Send only info about your device, its settings, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up-to-date, troubleshoot problems, and make product improvements."

You can see this for yourself by opening Settings | Privacy and clicking on Diagnostics & Feedback in the sidebar.

ADVANCED: (3 points)

Android safe mode: If, for some reason, you are unable to uninstall an app, reboot your Android device to Safe Mode . Go into your Settings app, open the list of installed apps, and remove any applications that might seem suspicious or malicious.

Remember, if your device has been infected with malware, your data may have been compromised. I strongly recommend that you change all your important credentials immediately, that is, change the passwords to your Google account(s), your banking credentials, and any other accounts that you believe may be affected.

Finally, if you still keep seeing ads and junk offers on your device, then you probably will need to factory reset your phone . Should you need to do this, I have TWO recommendations:

Backup all your data—your photos, documents, contacts, text messages, and many more—to an external storage device.

Instead of restoring your apps from the backup, reinstall them from the Google Play Store after the reset. You can use this as an opportunity to re-evaluate your app needs and only install apps as and when you need them.

I recommend the same for users who have rooted their Android devices, or jailbroken their iPhones.

Facebook

When you grant an app on Facebook the permission to read your profile, Facebook shares your unique Facebook ID; your first, middle, and last name; your picture; your email; and a list of the pages you manage freely with the app. In most cases, developers of apps will include broader permission requests as well, and ask you for your birthdate, your friends list, and your gender.

…and this is just the data that can be extracted WITHOUT human intervention!

Sandboxing

While most apps ensure that no sensitive personal information is allowed to leak out of internal storage, there may be instances where sensitive data might accidentally end up in the universally accessible external storage on your device.

For instance, you may download a bank statement and store it in your Downloads folder. Or you may download secret correspondence and save it in a text file in some folder on external storage. In both these cases, the downloaded files are accessible to you and also to any app that has the READ/WRITE EXTERNAL STORAGE permission.

Cambridge Analytica

If you are wondering why you should be worried about a bot that broadly sweeps available information, I have two words for you: Cambridge Analytica.

An academic researcher called Aleksandr Kogan developed a Facebook personality quiz app called This is Your Digital Life , which was used by a company called Cambridge Analytica to gather information on about 80 million Americans in 2014.

The exact data-points that were available to the app are not precisely known, but, based on freely available information on Facebook's Graph API, we can safely estimate that they definitely had access to (and almost certainly acquired information pertaining to) all of the following data-points for all users who took the personality quiz:

Table 2.1: A (non-exhaustive) list of the various data-points accessible to Cambridge Analytica through Facebook’s Graph API.

What made the whole thing worse was that the way Facebook permissions were designed, the app could access not just your information but also the information of all the people in your friends' list. So, even though only handful (estimated to be about fifteen hundred) users took the quiz, they (allegedly) ended up leaking details of around 80 million others.

Moral of the story? The next time you are invited to figure out which Marvel character you are, remember Cambridge Analytica, will you?

Info

“The Great Hack” on Netflix.

This 2019 documentary follows the Cambridge Analytica controversy in great detail—beginning with the shady methods used by CA to acquire profile data of users, right up to the investigations carried out by lawmakers in the US Congress and in the UK Parliament.

Cambridge Analytica collected about five thousand data-points to build accurate psych profiles for millions of Americans. They then were hired by various political clients (for example, Barack Obama, Ted Cruz, Donald Trump, Brexit, and many more) to promote stories on their Facebook timelines that subliminally encouraged them to vote in a certain manner.

To do this, they did not need to convince all of the voters in a specific geographical zone; they simply chose to convince only the number of people who were on the fence and swing their beliefs in the direction they wanted. Such people were called persuadables and the documentary goes into some amount of detail about how they were identified and categorized by an automated algorithm. I recommend you definitely watch it, whenever you get a chance.

All of your devices that are connected to the internet are constantly relaying various bits of identifiable information about you—information that can be merged and consolidated to create a larger picture of you and/or your life.

Of course, you could argue that these devices and services are trying to make your life easy by keeping a detailed track of your likes and dislikes. If that's what you believe, well, more power to you.

However, there might be some among you who are concerned about the amount of information being collected about you and your activities.

There might be some among you who would like some semblance of control over the information (and the huge amounts of it) that is being shared with various entities.

If you are one of these people I just described, then this book is exactly what you need.

BASIC: (1 point)

Prevention is always better than cure, so I strongly recommend that you do NOT download or store sensitive information to any folder on your external storage .

In case you do end up downloading sensitive information to your external storage, well, good luck. There is no way to know when the file was last accessed or which app accessed it. The most you can do is check which of your apps has been given the READ/WRITE EXTERNAL STORAGE permission and hope that none of them are malicious.

Adversaries and threats

All this while we've been discussing bots and programs (such as the one used by Cambridge Analytica, for instance) that are designed to automatically sweep information about you by casting a broad net.

Let’s raise the stakes a little bit. What if someone *specifically* wanted to find out information about YOU? Could they get their hands on it? What kind of information could they get their hands on? Something public? Something private? Would they be able to take advantage of this information?

The simple truth is this: Wherever there is private and/or personal data that requires protection, there will always be some kind of an adversary looking to acquire it in some unauthorized manner. With the introduction of internet-capable smartphones, the number of people accessing the internet has increased, and so has the number of malicious actors. Nigerian Prince scams are outdated; modern scammers can now employ much more sophisticated tools and techniques to con people.

In other words, adversaries on the internet have gotten a lot smarter. You need to be a lot more aware of them now than you were in the past. You need stay eternally vigilant and keep learning how to proactively defend yourself from any adversarial attacks on your private and/or personal data.

To do that, you need to understand who your adversaries are. So, let’s quickly look at a few common types of adversaries and/or threats that you might encounter on the internet.

Permissions

Even though the user now has greater control on the permissions being granted to each app, they are still vulnerable to the visual fatigue phenomenon—users grant their apps all the requested permissions, often blindly and mechanically. Apps use these permissions to collect and share all kinds of user metadata with their remote servers—we even showed you an example at the very beginning of the book, remember?

Passive adversaries

A passive adversary is someone who is not targeting you or your credentials but will gladly use your credentials to further act upon whatever malicious intent they may have.

Most 'hackers' on the internet can be classified as passive adversaries, since they look to acquire vast compilations of private and/or personal data without actively meaning to target any specific person. Also, since passive adversaries do not target you specifically, there is rarely any indication of your data being compromised until it gets used by an active adversary.

Note

There is a distinct possibility that your current email credentials, banking credentials, contact details, home address, etc. have already been accessed and sold by/to a passive adversary.

BASIC: (1 points)

Here are my recommendations to keep those permission-hungry apps under control:

Carefully evaluate every permission request made by an app instead of blindly clicking Allow every time the app prompts you to grant some permission.

Don't hesitate at all if you need to deny permissions to apps. Well-designed apps will usually explain why they need the permission.

Delete any apps that don't explain why they are asking for out-of-scope permissions, for example, a Flashlight app shouldn't be asking for location

permissions at all.

Review every permission that you have given an app by opening Settings| Installed Apps| Permissions .

As for Google's shady behavior with location permissions, well, here are a few different ways to deal with Google's overall disregard of the privacy of your personal data.

Use a privacy-focused search engine app such as DuckDuckGo or StartPage, instead of the Google app on your phone for searches. Use a completely separate Find my Phone app to circumvent Google's unwanted sharing of location permissions.

Active adversaries

An active adversary is someone who is specifically trying to gain access to YOUR private details.

Active adversaries make specific efforts to acquire any data that you may deem personal and/or private, such as your email credentials, your banking credentials, your home address, your contact details, and more. It is relatively easier to identify attacks by active adversaries than attacks by passive adversaries.

A passive adversary may (or may not) become an active adversary depending on whether (or not) they become specifically interested in you. Conversely, active adversaries may employ hacking techniques commonly employed by passive adversaries to get to your personal/private data.

INTERMEDIATE: (2 points)

Use a privacy-aware browser such as Firefox Focus, Brave, or Epic, and navigate to the duckduckgo.com webpage or the startpage.com webpage to execute your searches. Startpage, for instance, is built by a Dutch company and the search engine queries Google for results on your behalf. It also provides the Anonymous View feature to view the results anonymously.

Intrusive advertising

While intrusive advertising is considered by many as harmless, the Cambridge Analytica episode is proof enough that the data collected by advertisers can be weaponized to create psych profiles of individual users. A well-built psych profile can be used to manipulate users by feeding them information specifically designed to either alter or enhance their beliefs and perceptions.

Furthermore, intrusive advertising can also create false associations through incorrect marriage of collected data. A person searching for a tyre and a rope may not necessarily be looking to build a swing in their backyard, you know?

Invisible threats

Adversaries that are able to remain hidden before, during, or after an attack on your digital existence are what we classify as invisible threats.

This doesn't mean that such adversaries cannot be seen; it means that they may be so adept at covering their tracks that they are able to leave little to no trace of ever having existed. Hollywood uses the popular phrase 'ghost in the shell' to describe such invisible adversaries. Such adversarial techniques require significant knowledge and resources in order to ensure near-perfect execution. Typically, such knowledge and resources are usually available with either state actors or a handful of highly intelligent and dedicated cybersecurity professionals.

Note

While these categories broadly cover any potential adversaries you may encounter, this list is in no way neither exclusive nor exhaustive. More categories of adversaries may (or will) be discovered as we discover new ways of interacting in the digital world.

ADVANCED: (3 points)

Use a VPN to add another layer of security and/or anonymity to your browsing. A VPN or Virtual Private Network is an additional layer between you and the search engine, which allows you to mask your real IP address. Using a VPN is akin to playing Chinese Whispers—only more efficiently and without losing any information in the process.

Conclusion

Smartphone apps may have originally started off as curiosities, but they are now very much necessities. You cannot imagine travelling without Google Maps any more. You cannot imagine NOT having access to your email on the go. You cannot imagine not being able to exchange messages instantaneously with your loved ones. You cannot imagine NOT capturing a nice moment and sharing it with your friends and family.

In other words, smartphone apps are what make the smartphone, well, smart. Therefore, it stands to reason that they must be treated with utmost care and caution. You should never install apps of unknown origin. Sure, app stores usually take care to prevent malicious apps from reaching you, but, sometimes, carefully-crafted malicious apps may slip through the cracks. You still need to be the last line of defense on your smartphone.

It helps if you think of smartphone apps as a house that someone wants to give away for free. If someone made you such an offer, I'm sure your first question would be, What's the catch?

You need to ask the same question whenever you are about to install a free app. I suspect you are likely to find answers that you might not like.

---

[1] Remember the Flashlight app that needed location permissions? Yeah, that.

[2] Note the different types of ‘slash’ used for Windows PowerShell and MacOS—Windows uses the backslash, while MacOS uses a forward slash.

Chapter 6

Smart Devices and IoT

Introduction

When Steve Jobs demo-ed the first iPhone, the whole world was taken by storm and, right then and there, everyone knew two things for certain:

The market would soon be filled with BIGGER 'smart' devices.

The market would soon be filled with SMALLER 'smart' devices.

As of August 2019, we can safely say that BOTH these assumptions were right.

Since that historic day in 2007 (29th June 2007, to be exact) there has been constant innovation in the world of smart devices -- sometimes to the extent where one is forced to ask the question,"but why does THIS device need to be smart?"

Regardless, it must be noted that we live in a world where smart devices have now become extremely common and wide-ranging. These days, we see tiny smart devices, from fitness bands to mini-cameras, and we also see huge smart devices such as wall-to-wall smart TVs and refrigerators.

A wide variety of smart-devices is available for consumer usage, ranging from simple door locks without keys, to the more complex smart TVs and refrigerators, to the really quirky smart diapers, water bottles, hairbrushes, pregnancy test kit, candles or even sex toys!

Info

As you can see that not all smart devices are necessary, or even useful! Check out the

Tumblr blog, " We put a chip in it!" at https://weputachipinit.tumblr.com/ for some crazy examples of 'smart' tools and devices! Although many of these devices have now disappeared from the market, the very fact that they existed at some point is a good indicator of the kind of 'smartness' we have now come to expect from tools and utilities we use daily.

Note that smart devices do not necessarily need:

To be a handheld, portable, or wearable: They may be fixed in position and still be able to fulfil both the above criteria, for example, a smart refrigerator or a smart TV.

To have a touchscreen for interactivity: They may use other kinds of input. For example, smart speakers such as Alexa, Google Home, and many morerely on voice commands.

Some smart devices:

May use auxiliary devices for extended interactivity; for example, smart bands typically come with a companion app that connects with the smart band to exchange information with the app.

May be intended primarily for data collection and only provide rudimentary on-device interactivity, for example, the Nest thermostat by Google.

May exhibit some degree of artificial intelligence or machine learning by analyzing basic user behavior and compiling recommendations or suggestions for the user based on these analyses, for example, a smart speaker such as Amazon's Echo or Google Home.

So, what makes a smart device, smart ? I'd say that the two key features of smart devices are interactivity and autonomy:

Interactivity: Smart devices typically provide an interface for the user to issue various commands for operating them in a certain manner.

Autonomy: At the same time, smart devices have features that allow it to carry out certain automated tasks unsupervised.

For example, smartphones allow for a wide range of interactions and, at the same time, also execute automatic background processes that do not require any user input whatsoever.

These devices usually employ different wireless protocols such as Bluetooth, Wi-Fi, NFC, and many more, to connect with each other. They may also communicate with remote servers to accomplish more powerful and nuanced processing of data collected in the course of their usage. This ability to connect to other (similar) devices and operate (somewhat) autonomously is often commonly referred to as the Internet of Things (IoT).

The Internet of Things (IoT)

The most common example of IoT that is usually given is that of an automated smart home -- think Tom Cruise's character's home in Minority Report. Installing IoT-enabled devices provides Tom's character in the movie the ability to control several home utilities such as the entrance lock, lights, entertainment system, refrigerator, by issuing simple voice commands and/or gestures.

In the simplest terms, the IoT is a system of interconnected devices (each with its own unique identifier ID) that can communicate without requiring any human intervention whatsoever.

One of the earliest examples of an IoT-enabled device dates back to as early as 1982 when a vending machine installed at Carnegie Mellon University was modified to be able to report its inventory and temperature details on the contents of its freezer:

Figure 6.1: The ‘internet-connected’ vending machine installed at Carnegie Mellon University. (Image credits: https://www.engineersrule.com/how-a-coke-machine-and-the-industrial-internet-of-things-can-give-birth-to-a-planetary-computer/)

You can read the fascinating history of how this vending machine came to be on the official page of the Computer Science department of Carnegie-Mellon University, by visiting:

What we already know about you

I have a confession to make.

Remember, in the first chapter I asked you to scan a QR code and open a webpage. Well, I wasn't being entirely honest with you there.

https://www.cs.cmu.edu/~coke/

Alternatively, scan the QR code given alongside to open the page in a browser on your device. Although this page is no longer updated, it has been made available for historical reasons and provides a fascinating insight into the early days of IoT -- much before the term, IoT was even coined.

When you opened that webpage, you sent me a ton of data about you, your internet-connected device, your network, and a whole host of details about you that you probably didn't even know existed.

Don't worry, I am not going to use this data for any nefarious purposes – you have my word. In fact, if you want to see what data I was able to collect from you, simply scan the QR code shown alongside this paragraph and enter the alphanumeric code that you noted down (in the empty box) in the first chapter, earlier.

Alternatively, open your browser app and go to the following webpage:

https://leakscore.privacy.clinic

I just wanted to show you how much of your personal information is sent out there without you even knowing/realizing that you just gave it out. If you followed the instructions correctly (and if I was right in my assumptions), then I was probably able to correctly identify at least a few of the following:

Your mobile device make and model

The location where the picture was clicked (maybe)

Your preferred browser

Your location

Your telecom/internet service provider

Your physical location (maybe)

…and a few other things.

How would any of this help me, you wonder?

Well, some (or all) of this data, combined with your first and last name, would allow me to track down your social media profiles, which could possibly yield your birthdate. Using that, I could try and reset your email password, assuming you don't use any kind of Multifactor Authentication (2FA) on your email account.

If I am successful in gaining access to your email inbox, it could provide me with a plethora of valuable information, such as your bank account details, your secondary email address, not to mention your most frequently emailed contacts—in other words, names and email addresses of your loved ones.

Furthermore, if you are the kind of person who reuses the same email address for logging in to various sites, I could also try resetting the password to your bank accounts, and I get the feeling that I would probably be successful there as well.

…but you don't have to worry, I am not going to do anything of the sort. Scout's honor. I just wanted to give you a taste of how bad things could get, if you continued to remain careless.

In fact, how about you try it out yourself?

Come; let me guide you through the basics of snooping on yourself, using just simple search terms on Google.

Security vulnerabilities in IoT and smart devices

IoT devices have certainly come a long way since that simple vending machine and now find large-scale acceptance in our day-to-day life through several consumer-oriented applications such as smart thermostats, doorbells, locks, etc. and also through large-scale industrial applications in manufacturing, agriculture, and infrastructure development to name just a few.

The IoT can easily encode (that is, track and follow) between 50 to 100 trillion objects and it is expected that the world will have close to (or even

more than) 200 million IoT devices by 2020.

As you may have realized by now, this behavior goes against the three fundamental rules of privacy that we have outlined earlier in the book. There have been multiple instances of vulnerabilities being discovered in various smart devices which were then subjected to subsequent exploitative attacks. The following section contains some of the more famous examples of IoT devices being breached:

The basics of snooping

Let's start with a simple search on Google.

Say, you are one of those people who have a rather common name, for example, Amit Sharma or Rajesh Patel . The search results page is obviously going to throw up a lot of results. That is, however, not a problem. Simply add site: facebook.com to your search terms, that is, instead of searching for Amit Sharma , we'll now search for Amit Sharma site:facebook.com.

Note

I'm deliberately choosing the name Amit Sharma here because Amit is one of the most common Indian names and Sharma is also a very common Indian surname. To any Amit Sharma's that may be reading this, my apologies, I didn't mean to target you specifically!

What we're telling Google here is something along the lines of; Show me only the results for Amit Sharma which has come from facebook.com. Typically, the first result from Google will be a link titled Amit Sharma Profiles with a link such as:

https://www.facebook.com/public/Amit-Sharma

Okay, this tells us that there a LOT of Amit Sharma's in the world! It will take us ages to scroll through all of them and identify them by their photos! Let's see if we can narrow the results by tweaking our search terms a little bit. Let's add in the city where you live to the search term, that is, let's search for Amit Sharma Pune site:facebook.com.

Most of the time, these two steps are enough to identify a relevant Facebook profile—in this case, YOUR Facebook profile. Open this profile in an incognito/private window to see what information is being made publicly available by facebook.com to the world.

For instance, in the case of Amit Sharma from Pune, you'll notice straightaway that Facebook immediately tells you where the person works, where they have studied, what their 'likes' are, etc. It even helpfully lists other people with the same name in case this is not the profile you are looking for.

…and that's just in the incognito window!

Someone who is logged into Facebook and on your friend list will, obviously, be able to acquire a lot more information by accessing the various tabs on your Facebook profile, that is, About, Friends, Photos, and (ironically) more. In some cases, I have been able to find birthdates, addresses, and even mobile numbers and email addresses on the About tab itself!

Strava

Strava is an app primarily aimed at athletes -- specifically runners and cyclists, and it shows the most popular routes for running and cycling. The Strava app can be synced with multiple smartphones, monitors, and fitness trackers, to record various performance metrics of its users.

Advanced snooping or OSINT

OSINT , short for Open Source Intelligence , refers to the practice of uncovering valuable information about a particular target using openly available data.

This image posted on a blog post titled, The Ultimate List of 50 Free Security Tools, Tested For You on the Heimdall Security Blog, gives a good idea of how a complete picture can be derived by systematically searching/accessing information from various online sources:

In 2017, the Strava released a data visualization map, with more than 3 trillion individual GPS data points, that showed a heatmap of all activities uploaded to Strava by its users. However, soon after the visualization map was made public, military analysts realized that it (the map) was detailed enough to inadvertently give away locations and movements of military personnel, who also happened to be users of Strava.

For more details, check: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Figure 2.1: Various online sources for sourcing OSINT information (Source: https://heimdalsecurity.com/blog/free-cyber-security-tools-list/)

Note that some of the sources mentioned in the image may not qualify as freely available, but the image still manages to provide a good idea of how OSINT works.

Coming back to our example, using only a name, city of residence, and the knowledge of what someone looks like, (in this case, that someone being you), I was able to help you track down your Facebook profile. The profile page would further yield crucial information, such as workplace, education details, and a bunch of other information that can be further used to identify relevant profiles on other social networks in future searches.

…and we haven't even opened Twitter, Instagram, or any of the other social networks yet!

Acquiring your address isn't very difficult either…

Imagine receiving the following call:

"Hello, is this Amit Sharma? Congratulations! You have won a toaster in our lucky draw! Which lucky draw? Well, every month, we reward a few lucky customers who purchase from Flipkart! Could you please confirm your date of birth and your postal address to ensure that we have got the right Amit Sharma? It is such a common name, you know?!"

…or alternatively, getting this SMS:

"Congratulations, Amit Sharma! You have won a toaster from Flipkart! To get your prize delivered, please WhatsApp a copy of your ID and address proof to +91 98XXXX XXXXX within 24 hours of receiving this SMS."

Sure, you may be smart enough not to fall for this scam, but these examples were just a way to illustrate how easy it is to acquire your home address through a simple phone call or SMS. A smart adversary will probably even carefully customize the pitch in a manner that will sound completely believable.

Smart TVs

A study by Consumer Reports in 2018 found that millions of smart TVs were susceptible to attacks by malicious actors. A malicious actor who gained control could turn up the volume, rapidly switch through channels, open disturbing content, and disconnect the TV from the Wi-Fi network. Thankfully, this specific vulnerability did not allow the malicious actor to extract any private information, or monitor what is being played on a smart TV. The QR code given alongside this paragraph links directly to the study published by consumer reports, in case you wish to read it for yourself.

Conclusion

I want to clarify something here: My intention in this chapter is not to alarm you.

That said, if this chapter alarmed you, good. As wonderful as the internet is, it is also a place where we unknowingly give away tons of information about us. The examples I outlined in this chapter have convinced you just how easy it is. If you still don't believe me, think of the first person you met today. Now, use the techniques I followed in this chapter and see how quickly you can figure out the following details:

Their full name

Their date of birth

Their postal address

Their email address

Their mobile number

So, how long did it take you? Not very long, I presume?

Here's the thing, if this little example above has served as a wake-up call of sorts for you, then this book is exactly what you need. Sit down with your smartphone, or your PC, or your smart device, and make the changes that I recommend at various points in this book. Make the effort to secure your data.

I am not going to promise that this book is a silver bullet for all your security needs.

Security and privacy isn't a solution that you can implement—it is a lifestyle that you must adopt. I am here to teach you a lifestyle, if you are willing to put in the effort to learn it.

Are you ready?

[QRCode: https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/]

A specific exploit for Samsung's F-series smart TV was designed by the CIA jointly with MI5, in June 2014. It was called the Weeping Angel attack (released in the Vault 7 leaks by Wikileaks), and it allowed anyone with physical access to these Samsung Smart TVs to installing a malicious firmware. This malicious firmware would pretend to put your TV in a fake 'off' mode but would remain on and could record all the audio, and upload it when it was switched back ON. The QR code given alongside this paragraph will lead you to a page on Wikileaks describing the Weeping Angel attack in detail.

Section 2

Devices

[QRCode: https://wikileaks.org/ciav7p1/cms/page_12353643.html]

Moreover, almost all of these smart TVs have extremely overarching privacy agreements, in which you are (almost) forced to consent to wide-ranging data collection by the makers of the various apps and/or the TV itself. Scan the QR code given alongside this paragraph to read more about the various vulnerabilities in Smart TVs that have been exploited until now.

Chapter 3

Android Devices

[QRCode: https://hackaday.com/tag/smart-tv-hack/]

Introduction

All smartphones -- be it an Android, an iPhone, or a Windows [1] phone -- leak data.

If you are using an Android-based (or Android-equipped) phone, your phone might be sending tons of data back to Google -- often, without your knowledge and/or consent. If you're using an iPhone, it is probably sending data back to Apple -- although not as much as Google, I believe.

To be fair, the entire Google ecosystem is designed to aggressively collect data about your interests and show you ads that are most relevant to your interests. In contrast, Apple labels itself a product company and has strongly distanced itself from any and all privacy-intrusive data collection.

So, which of them is the better option?

Over the next few chapters, we'll be enumerating the various privacy issues in smartphones and how to deal with them. We'll begin with the Android OS and then look at iOS separately [2] , and finally look at the apps on your smartphone that might be sharing crucial information without your knowledge and/or consent.

Alexa, Siri, and Google

Maybe, it is due to the novelty of being able to talk to them or maybe it is the slight superiority one gets to feel while ordering them around but voice-activated tech has gotten increasingly popular with consumers over the last few years. Amazon's Alexa, Apple's Siri, and Google's Assistant have found themselves being increasingly tightly integrated with the various gadgets being sold by these tech companies.

What most buyers of these gadgets don't realize is that everything you that is said to Alexa, Siri, Cortana, or Google's Assistant is sent to the respective servers for processing purposes. The processing, in this case, involves converting the speech to text, parsing the text for commands, and sending back an appropriate response based on the command.

Furthermore, this processed audio doesn't get deleted immediately.

Sure, the tech companies claim that your audio gets encrypted in transit and is always stored securely in the cloud BUT did you know that the staff assigned to improving the speech-to-text accuracy for these devices is given access to a select subset of people's private recordings?

An April 2019 investigation by Bloomberg revealed that a specific mix of people hired by Amazon (which includes both employees and contractors) were assigned to listen to these audio recordings and annotate them for training the speech recognition software. In fact, on some occasions, some of the recorded audio was found to be inadvertent, that is, the voice-recognition software wrongly interpreted random sounds like the wake word and accidentally recorded entire private conversations that were then uploaded to the cloud, where they were then (in some cases) heard by these subcontractors.

In other words, some of the machine-learning and artificial intelligence displayed by these devices may possibly have had a human intervention and, as a result, some private details may have been heard by people that it was definitely not intended for.

The Google-Android ecosystem

We know that the Android OS is developed and maintained by Google. However, that should not be taken to mean that Android is Google or vice-versa. Android is just a product developed by Google, and it uses a lot of Google's services. However, these services are not necessarily required or mandatory for running Android on a compatible smartphone.

Confused? Well, let me explain…

While Google does have a significant presence on Android-equipped and Android-enabled smartphones, it does not mean that Google develops everything in the entire Android ecosystem. In fact, many phone manufacturers prefer to adapt the Android OS to their own brand and create something different.

To understand this somewhat complicated relationship, imagine AOSP as the engine of a racing car. Google also, incidentally, happens to be the manufacturer that produces other essential car parts such as the steering, transmission, wheel, tires, internal wiring mechanism, and more.

Each racing team (that is, phone manufacturer) has the freedom to build their own chassis (that is, handset models) and slap their own livery (that is, user interface) on it to manufacture their own custom version of an Android-based machine -- think Red Bull using Ferrari engines or McLaren using Mercedes engines in F1 races.

At the heart of it, these phones still run on Android and the internal mechanisms are still provided by Google, but each racing team is free to make additions as they please. Some merely change the livery (for example, Samsung and HTC) while others make changes to the internal wiring (for example, OnePlus and Xiaomi) before selling the machine to customers.

In case you were keeping track, this makes the Google Pixel [3] phones the (closest) equivalent of a stockcar since it runs the AOSP engine (which is developed by Google) and all essential parts and livery are designed by the same manufacturer that manufactures the engine , viz. Google.

For example, the TouchWiz UI on most Samsung phones is mostly an enhancement of the stock Android UI, but Samsung also includes a few exclusive third-party Android apps with its phones. Other phone manufacturers may choose to make far more comprehensive changes, for example, MIUI OS on Xiaomi phones. Not only is the MIUI OS designed to (somewhat) emulate the iPhone user interface; it also collects a staggering amount of data. This data is then processed to show us relevant advertisements in the form of Suggestions and Recommendations *within* the OS itself!

This analogy holds up well with upgrades too.

Like all engine models undergo improvements from time to time, so does AOSP. If you wish you can choose only to buy the latest model (that is, buy the new Google Pixel). The teams can choose to upgrade just the engine, or make cosmetic changes, or design a completely new chassis, or maybe even do everything at once.

All of this is singularly possible, thanks to the Android Open-Source Project(AOSP).

Smart appliances

Do you think your refrigerator could snitch on you? Do you believe your thermostat could kill you? Or hold you to ransom? Or your doorbell? If I told you, your toaster might have participated in breaking the internet, would you believe me?

Well, each of those situations is entirely possible and, in fact, has happened.

In 2015, a team of hackers managed to exploit a smart refrigerator to reveal the Gmail credentials associated with the calendar that was being displayed on the screen of the fridge. The same people also managed to exploit a smart thermostat, gained control over it and displayed a 'ransom message' on its screen.

Later, in 2016, Russian hackers unleashed a botnet that exploited the weak security of IoT-enabled devices (such as your toasters, security cameras, baby monitors, and many more) in a worldwide DDoS (Distributed Denial of Service) attack that took down a bunch of sites on the internet, including The New York Times, Reddit, Twitter, Spotify, PlayStation, Paypal, and many others.

Android Open-Source Project (AOSP)

Here's how the official Source website describes the Android Open Source Project or AOSP:

Android is an open-source software stack created for a wide array of devices with different form factors. Android's primary purpose is to create an open software platform available for carriers, OEMs, and developers to make their innovative ideas a reality and to introduce a successful, real-world product that improves the mobile experience for users.

— (https://source.android.com/setup/ , as on July 20, 2019)

Simply speaking, AOSP isn't a complete OS by itself; it is merely the platform on which the rest of the Android OS is built. Anyone can use this platform and build something else entirely on top of it, while still calling it Android.

Remember what I said earlier?

AOSP is the engine and the various applications and services provided by Google are the essential components (steering, transmission, wheels, tires, internal wiring, and more.) that make up the basic skeleton of the car.

These applications and services that Google provides actually have a name – they are called Google Mobile Services (GMS). According to the Android – Google Mobile Services page: (https://www.android.com/gms/)

While the Android Open Source Project (AOSP) provides common, device-level functionalities such as email and calling, GMS is not part of AOSP. GMS is only available through a license with Google and delivers a holistic set of popular apps and cloud-based services.

[QRCode: https://en.wikipedia.org/wiki/2016*Dyn*cyberattack]

It is estimated that there are readily available botnets that can deploy more than three lakh IoT-enabled devices to unleash a DDoS attack at any given target.

However, that's not the scary part. The scary part is this:

Your IoT-enabled device may already be compromised. It might even get used as a part of a massive botnet in a future DDoS attack -- that means one (or all) of your IoT-enabled devices may be partly responsible for a future DDoS attack, and you won't even realize it!

So, why does Google do this?

To put it simply, AOSP is Google's way of maintaining a viable alternative to its biggest competitor in the market – Apple's iOS. By making the AOSP free to use, Google ensured two things:

Cheaper smartphones: Every smartphone manufacturer – past and present – had an inexpensive (read: free) option for an - operating system to put on their smartphone hardware. This meant that companies could make and sell Android-enabled or Android-equipped smartphones for far cheaper than Apple iPhones.

More Google/Android users: The more the people buying Android-enabled or Android-equipped phones and devices, the more the traffic for Google and its products and services.

You see, Google develops and maintains the Android source code, that is, keeps it clean and tidy, keeps it up-to-date, and makes it available for people/organizations who might want to use it.

Of course, Google does all of this under a very liberal license that allows different people to utilize the code differently, according to their needs. That means, Samsung can tweak the code to bundle in their TouchWiz UI and Xiaomi can tweak it to give their users, their heavily modified version, that is, MIUI.

However, it also means that Google gets to decide the direction the AOSP takes. They get to decide what features are to be developed and incorporated into AOSP and by extension the stock Android OS. It also means that Google can tweak AOSP to include the code necessary to collect whatever data they wish from people who just happen to be using some version of the Android OS – stock or otherwise.

RohitRecommends

I cannot deny that we are headed towards a future where all technology is connected, and all devices are capable of speaking to each other. At the same time, I feel it is important to keep track of what information is being shared between these devices. Choosing to ignore this puts us in a situation where we can be affected (or even harmed) by the information asymmetry thus generated.

The recommendations we have chosen to propose are, thus, based on the following guiding principles:

Knowledge of information-sharing, that is, being aware of what information by devices, is being shared and who has access to it, at all times.

Knowledge of interference, that is, having the ability to make changes to the quality and quantity of information being shared, at any time.

Execution of interference, that is, taking concrete steps to actually make changes to the quality and quantity of information being shared, whenever and wherever deemed necessary.

Using these guiding principles, we’re going to figure out a suitable system to deal with the privacy issues that may arise from the usage of smart devices.

What is a ROM?

In the world of Android, ROM refers to the read-only part of internal storage, which contains the operating system.

The read-only attribute of the internal storage ensures that no changes that can cause the device to malfunction can be made. These official ROMs are also called firmware sometimes since the software stays firmly in place, that is, regular device users are not allowed to make any

modifications whatsoever.

Info

Why are they called ROMs?

The term 'ROM' comes from the era of CDs and DVDs -- technically called CD-ROMs and DVD-ROMs, respectively. The ROM in their names stood for Read-Only Memory, that is, the memory that cannot be erased or rewritten.

However, in case of Android, modification of firmware/official ROM is not impossible -- the only deterrent in most cases being a software or hardware lock. Hardware locks require specialized devices to unlock them, whereas software locks can be overridden by using special software written for the express purpose of performing this task.

Official ROMs

Official ROMs or firmware are usually of two varieties:

The Google Android OS commonly referred to as Stock Android

A customized Android commonly referred to as Firmware

Only a select few devices ship with the stock Android OS, such as the Google Pixel series, Nokia 6 and 8 series, the Xiaomi Mi A-series, and more. In most cases, manufacturer-branded firmware often has some enhancements added over the stock Android OS. These enhancements range from simple interface enhancements to severe usage restrictions.

Sometimes, firmware may be customized and branded either according to the manufacturer or the telecom service provider. In rare cases, your device may have firmware that has been customized by BOTH manufacturer and the telecom service provider, although this is mostly a US thing. Most Indian telecom service providers do not offer such locked devices -- customers are free (and often encouraged) to purchase their own devices.

In some extreme cases, the customizations to the stock Android OS maybe so substantial that an argument can be made about them being more of custom ROMs, rather than manufacturer-branded firmware.

BASIC: (1 point)

Regardless of what you think about smart devices and the IoT, it is extremely critical that you know and understand the length and breadth of data-sharing that these devices indulge in. That means, having full knowledge of what data is being shared and who (potentially) could have access to it.

Most devices require companion apps to be installed, and these companion apps may or may not collect additional data, on top of the data collected by smart devices. You need to be fully aware of all the data that is being collected in both cases – the companion app, and the device itself. You also need to understand and accept the implications of this data being sent over the internet to be stored in remote servers.

Once you are equipped with all of the knowledge outlined above, you must weigh it against the potential benefits being offered by the smart device and the enhancement in the quality of life that the device brings and ask yourself the questions:

"Can I (or, do I) use this smart device regularly?"

"Does this service offered by the smart device (and its companion app) merit sharing all of this data about me in exchange?" (Remember the butler?)

"If/When I stop using this device, is it likely to affect the quality of my life negatively?"

If the answer to any of these questions is No then you might want to proceed further. If not, then you may safely skip the rest of this section and proceed to the next chapter.

Custom ROMs

Thanks to AOSP being open-source, many independent developers have attempted to customize the OS in very specific ways for their favorite devices by making modifications to the source code. These developers often tend to release their tweaked code for the general public to use as custom ROMs.

In simple words, a custom ROM is an 'unofficial' firmware for a specific phone made by some independent developer(s) that has been released to the general public.

Some popular custom ROMs that are available for a wide variety of devices are Lineage OS, OmniROM, Replicant OS, SlimROM, Paranoid Android, Resurrection Remix, and AOSP Extended.

Info

The very first piece of tech that Xiaomi (the phone manufacturers behind 'flagship-killers' such as the Redmi Note 5 and the Pocophone F1) released was actually a custom ROM for several popular Android phones called MIUI, back in August 2010. A year later, the Xiaomi Mi 1 smartphone was announced. The developers of CyanogenMod, another popular custom ROM, had a deal with OnePlus for a while. However, that deal ended after OnePlus decided to ship their phones with OxygenOS instead. CyanogenMod goes by a different name these days; you probably know it as LineageOS!

XDA, the go-to forum for all things Android, has a detailed post describing the most popular custom ROMs for Android phones, here:

https://www.xda-developers.com/the-most-popular-custom-roms-on-xda/

Scan the QR code given alongside this paragraph to read a quick overview of the most popular custom ROMs on the XDA forums.

INTERMEDIATE: (2 points)

Equipped with the knowledge acquired in the previous (Basic) section, we invite you to evaluate your position a little more rigorously here. The questions you need to ask yourself at this stage are:

"Do I absolutely WANT to use (or to continue using) this device?"

"Am I okay withthe data that is being shared by the device and its companion app?"

If you answered No to any of the questions, then your answer is clear: You need to stop using the device right away. You need to switch it off, delete the companion app, delete any public accounts or identities you may have made in the process, delete the data stored on the smart device and the remote servers, and forget that the device (or the companion app) ever existed in the first place. You may then skip to the next chapter.

If you answered Yes to BOTH the questions, then you might want to read further, that is, the Advanced section.

ADVANCED: (3 points)

We do NOT recommend doing this unless you exactly know what you are getting into. Please ensure that you have expert supervision/consultation when you attempt this!

It is possible to use the smart devices and their companion apps in a manner that insulates the data being sent by them from the rest of the traffic on your network. This, however, requires significant technical knowledge and expertise of computer networks and internet traffic monitoring. You can find detailed guides on the internet by searching for appropriate keywords, such as Isolating [SMART DEVICE NAME] on Home Network or something similar.

Here’s a broad explanation on how this is done:

Create a separate (hidden, maybe?) secondary network for your smart devices.

Ensure that this network is properly firewalled and that it does not leak into your primary network.

Use this network (and only this network) to connect smart devices to the internet.

Use a separate smartphone/tablet for the companion app, and use the secondary network to access the internet on this smartphone/tablet

If you’d like, you can install an additional VPN to create a secondary layer of separation between the network and the internet.

EXPERT: (5 points)

I only have two specific recommendations here:

Stop, I repeat, STOP using smart devices and/or IoT.

Do not; I repeat, DO NOT use any smart devices or IoT-enabled devices.

Official firmware vs custom ROMs

Unlike stock firmware, custom ROMs can be notoriously unstable. However, custom ROMs are also developed and tested at a rapid pace, with some popular custom ROMs even pushing out updates on a nightly basis!

On the other hand, stock firmware goes through rigorous testing and scheduled release cycles. However, this also means that updates may take a long time to ultimately reach end-users -- especially if they live outside of the continental United States.

Given below is a table that shows the major differences between official firmware and custom ROMs. Note that this table covers most of the major differences but should, in no way, be considered exhaustive:

Table 3.1: A non-exhaustive comparison between official firmware and custom ROMs.

Based on this table, one might feel that rooting your phone and/or installing a custom ROM is the smartest thing you can do with your Android phone. However, before you do that, remember that installing a custom ROM might void the warranty on your phone. Think carefully and evaluate whether you really need to install that custom ROM on your Android phone before you decide to go through with this decision.

Android and privacy

Google constantly strives to make Android a secure OS. However, the open nature of the platform means that developers of various Android ROMs (both manufacturer firmware and custom ROMs) can attach additional programming to their ROMS to compromise the privacy of your personal data.

Most manufacturers claim that they are actually providing a service by allowing users to retain cloud-based backups of their data. However, that makes these backups immediately vulnerable to malicious actors, who might try several illegal methods (discussed in the previous chapter and throughout this book) to acquire this data.

This is not to say that people with Android-based or Android-equipped phones cannot hope for privacy. Like with all other things, it is difficult but not impossible.

In the following sections, I will outline some of the privacy concerns and then explain what you can (or rather, must) do to mitigate them and regain control over your personal data and how it is shared.

Conclusion

Smart devices and appliances definitely have their uses. They provide us with services that attempt to make our life easier. However, until their security is strengthened, they will continue to remain a liability rather than an asset.

There are products available in the market that will help you protect your IoT-enabled devices from intrusions. There are steps you can take yourself to mitigate such attacks and to ensure that your smart devices do not get captured into a botnet. There are ways to ensure greater security for all the devices in your network.

However, there is only one guiding principle that I will advise to everyone who wishes to use any smart devices: If there is some information you don't want to share with the world, make sure that any and all of your devices do NOT have any access to that information. That means either isolating that information from the rest of the world or isolating all your devices so that they do not have direct access to that information.

Regardless of which option you choose, you will have to ensure that this status quo does not change. Ever.

Google Telemetry

Let's make something perfectly clear: Google is in the business of collecting your data. If in the process, they have to give something away for free, they are very likely to do it and often without a second thought.

Google still makes most of its money by serving contextual ads on webpages, i.e. ads that are relevant to you AND the webpage you are viewing. That's why you might see ads for shoes on a webpage on your device, but your wife might see ads for jewellery on the same webpage on her device. To decide which ad to display for a particular user, Google collects information from its various 'free' products and offerings.

Thus, every time you open Gmail, search for directions on Google Maps, watch a video on YouTube, search on Google, view a webpage in Google Chrome, read documents in Google Doc, listen to a podcast episode in Google Podcasts, upload files and photos to your Google Drive, connect to your car entertainment system with Google Auto, cast your screen using a Chromecast, call someone using Google Duo, download an app on the Google Play Store, translate stuff using the Google Translate app, you are sharing a lot of information with Google.

Info

Did you know, in 2014, Google bought a smart thermostat-manufacturer called Nest for $3.2 billion in cash?

Nest (at the time) made smart thermostats and smoke detectors that could speak to each other and to other Nest devices across the internet. Google, at the time, was primarily in the business of displaying ads to users across the internet. So, the question that arose was obvious?

Chapter 7

Desktops - Operating Systems

So, why was Google interested in the Nest? Was Google planning to broadcast ads on their tiny smart-screens?

Actually, the data these devices were gathering was just the beginning of the revolution we know today as IoT - the Internet of Things. Google had realized that by gathering information about how you used various appliances at home, they could create a more complete profile of you. In fact, in Feb 2019, Google confirmed in that Nest has a hidden microphone but it had erroneously omitted it from its tech specs.

If you are thinking that they were going to use this profile to serve you with more contextual ads, you would be absolutely right…

In fact, if you want to know what information Google stores about you, simply visit the following link:

https://takeout.google.com/settings/takeout

…and download your data. In fact, here's a handy QR code that you can scan, which will take you straight to the Google Takeout page.

Go ahead and scan it. Trust me; you'll be surprised at the length and breadth of information Google has about you.

Introduction

Regardless of how many smart devices we own, we still use desktop computers and/or laptops on a daily basis. In fact, quite a few of us use separate machines for home use and office use. It is extremely important to ensure that you maintain the highest level of security for both these machines since they are quite vulnerable to a range of adversarial attacks -- especially those that are connected to the internet, which is probably all of them.

Typically, the average user will use at least one of the following three kinds of PCs during their lifetime:

Home computer

Work computer

Unknown computer

Now, the first two categories are pretty much self-explanatory. The third category, (that is, Unknown computer) refers to all computers that do not fall under the first two categories. Thus, computers at a cyber-café, computers that you borrow from someone, computers you inherit – basically, any computer that has not been purchased and set up by you personally (or your office) will be classified as an unknown computer for purposes of this book.

Obviously, you cannot guarantee that your data will remain secure and private on any machine other than your own -- not even your work computer since your IT department gets to decide administrative policies for that computer. However, there are ways in which you can still ensure the security and privacy of your data on such computers, too. As with most devices, you have a wide range of options for securing such computers; you can secure them just enough or a lot, depending on how careful (maybe even, paranoid) you want to be about your data.

In the following sections, we'll take a look at the various machines you are likely to access and how to go about ensuring the security and privacy of your data on each one of them.

Non-Google Telemetry

All manufacturers who customize AOSP for their respective devices indulge in attempts to collect user data from Android devices, even Google. In

fact, the stock Android OS itself has a ton of telemetry options that relay various bits of information back to Google servers.

With non-Google manufacturers, devices may send a lot of telemetry data to servers, sometimes, outside the home country -- depending on where the device manufacturer chooses to install these servers. This data may or may not be scrubbed; that is, it may still contain elements that can be used to identify you, thereby rendering your privacy compromised personally.

Operating systems

The operating system is the primary agent that connects you to the rest of the internet. Programs on your system use the operating system to acquire your input, analyze your input, access the underlying hardware, perform various tasks based on your input, and present you with results.

It stands to reason, therefore, that having a privacy-aware operating system should be extremely important since the operating system can 'see' everything you do on your computer.

In case you are wondering, no, you can't turn this off.

Since the operating system needs to interact with various parts of the system, it must have access to them. If it has access to them, it can (and must be able to) examine all of these parts. If it can examine all of these parts, it can also keep a detailed account of everything that is happening with the system. There is no turning this off without interfering with the core working philosophy of the operating system. The best you can do is trust the operating system (and its developers) to not share this information with anyone else without your knowledge and consent. The notion of privacy and security when dealing with operating systems is, this, largely predicated on one factor – trust.

At the same time, you can (and must) take steps to ensure that you do not end up sharing this information with untrusted parties -- either by accident or on purpose -- which means, you will need to adopt a more secure, more privacy-aware approach with regards to your digital behaviors. In other words, to use the old cliché:

Trust no one, not even yourself.

In the sections that follow, we'll take a look at the various privacy and security issues that can arise while using various operating systems on a day-to-day basis. We'll look at enhancing user privacy by securing your accounts, by controlling the various (baked-in) telemetry options, and by carefully inspecting the applications installed on the system.

OnePlus Telemetry

In 2017, a security researcher named Chris Moore found that OnePlus phones were sending sensitive user data back to Chinese servers without permission. Subsequent investigations revealed that users had found traces of similar behavior on their older OnePlus devices going as far back as 2016.

When the story broke, OnePlus apologized and made changes to how their devices collect data and made the whole thing an opt-in, by calling it the User Experience Program .

Microsoft Windows

Since its release in 1985, Microsoft Windows has gone from strength to strength as the operating system of choice for the average PC user. In spite of facing tough competition from rival Apple from time to time, Windows has blown the competition away thanks to its user-friendly interfaces and adaptability to most modern hardware. While Apple insists on providing fully integrated machines, i.e. machines designed for immediate personal use, Windows is often preferred by people because it allows for a wide range of customizations -- something Apple doesn't provide with equal ease.

Thanks to the licensing model adopted by Microsoft, the Windows operating system can be installed on a variety of devices built by several PC manufacturers such as Dell, HP, Toshiba - to name just a few. Savvy enthusiasts can build their rigs as per their requirements, mixing and matching various components to suit their specific needs. Gamers can build PCs using configurations with powerful graphics cards, while people-on-the-go can choose PCs (laptops) with longer battery life, and home users can choose something less expensive to fit their budget. Windows has been proven to run on most, if not all, of these configurations without a hitch, which makes Windows the OS of choice for most people.

As of January 2019, according to Statista.com, Windows had around 75% of the market share when it came to operating systems on personal computers. It is also worth noting that Windows has remained a dominant presence in the personal computer operating system market and that their market share has never dipped below 70% since 2013. In India, according to Statcounter.com, Windows dominates the market with around 80% of the market share, as of June 2019. 46% of Indian Windows users run Windows 10, 43% run Windows 7, and all the other versions of Windows make up the rest.

Clearly, Windows 7 and Windows 10 are the OSes of choice for Indians. Therefore, in this chapter (and the chapters that follow) I've chosen to focus a majority of my discussion and evaluation around these two choices.

However, its popularity also makes Windows the primary target OS for hackers and other malicious actors, which is why most malicious software affects Windows more than it does the other two OSes, viz. macOS, and Linux.

Note

It's not true that they (macOS or Linux) don't have viruses; it's just that there is little interest in spending significant resources in developing viruses, malware, and other attack vectors for an OS that has barely 14% of the worldwide market share. If anything, the argument that macOS/Linux doesn't have viruses applies only due to the disinterest of the attackers rather than actual vulnerability issues.

In any case, the fact that Windows has such a large attack surface means that we need to be extremely careful about ensuring that our data is private and secure when using this OS.

Xiaomi Telemetry anddata breach

It was suspected that Xiaomi phones were sending critical private information (such as the IMEI numbers, address books, and messages) to Chinese servers. These suspicions were revealed to be true in 2014 when an independent Taiwanese researcher found a critical security flaw in the Xiaomi website code that exposed a ton of user details. The researcher claimed that he could access the credentials of millions of Xiaomi accounts and logs from the servers.

Xiaomi investigated the claim and subsequently issued a statement denying both the vulnerability and the leak. They counter-claimed that the data being claimed by the Taiwanese researcher was from 2012 and not 2014 as was being claimed. It was also obsolete since they had switched to a different account system.

To their credit, however, Xiaomi immediately asked their users to reset their passwords and publicly announced the incident as a way to mitigate any potential fallout from this incident.

Modern Windows (Win10, Win 8.1, and Win8)

Three years after the release of Windows 7 in 2009, Windows 8 was made available to the general public in October 2012, with Windows 8.1 following a year later in October 2013.

Both of these operating systems were received rather critically by the users, because of the sudden shift in the design, as compared to Windows 7. Many users across the internet reported the absence of the traditional Start menu and taskbar as being one of the major drawbacks of the new version of the operating system. Noting all of these concerns, Microsoft launched Windows 10 in July 2015 and gave licensed users a full year to update straight from Windows 7 to Windows 10 for free.

The strategy seems to have worked since Windows 10 is now reported to have a 58% usage share of all Windows versions on traditional PCs (with Windows 8 and 8.1 accounting for a combined 7.5%) as of July 2019. (Source: StatCounter Global Stats, Desktop Windows Version Market Share Worldwide).

…and others!

Around the same time as the Xiaomi story broke, Sony Xperia phones were also found secretly transmitting user-data to Chinese servers using similar spyware. There have been several reports over the last few years of other well-known Android devices [4] phoning home as well.

[QR Code: http://gs.statcounter.com/windows-version-market-share/desktop/worldwide/]

Windows 10 operates on the OS-as-a-service model, meaning that features and updates cannot be selectively installed but instead are delivered and installed without any user intervention. In simple words, if you have Windows 8 or below, I would recommend that you upgrade to the latest version of Windows 10, as soon as possible.

Recommendations and suggestions

You may have noticed some variation of Recommended Apps or Suggested Apps being displayed on your non-Google Android phone. Some of these may be due to an adware-infected app, while others may be due to the firmware or the OS itself!

Xiaomi, for instance, has recently been found to be inserting advertisements in the OS itself. In its most recent OS update for its phones, that is,

MIUI v10 recommended apps were spotted in at least eight different places in the OS. Xiaomi subsidizes the cost of the phone by providing these recommendations , which are usually paid for by creators of the app or service being advertised.

In other words, they are leasing out advertising space on your phone, and they are doing so without your permission.

Huawei, Honor, and a few other lesser-known phone manufacturers have also been caught pushing lock-screen ads on the devices of unsuspecting users in the past. Both Huawei and Honor have since made changes, and the ads are no longer visible on their devices.

Windows 7 and older versions

Windows 7 was initially supposed to be an incremental upgrade to Windows Vista, with tweaks made to improve hardware and software compatibility. However, continued criticism of Windows Vista resulted in Microsoft deciding to provide Windows 7 as a standalone version of the popular OS.

The decision worked in Microsoft's favor, with 100 million copies being shipped worldwide in just six months, increasing to over 630 million licenses by July 2012. As of July 2019, an estimated 32% of computers running Windows still run on Windows 7.

However, mainstream support for Windows 7 ended on January 2015, and extended support for Windows 7 ended on January 14th 2020. Users of Professional and Enterprise versions of Windows can opt to purchase Extended Security Updates that will offer additional updates for three years after extended support ends, that is, until 2023.

Sensors

In addition to your GSM/CDMA and Wi-Fi radios, most modern phones these days are equipped with a variety of sensors such as GPS, Bluetooth, Near-Field Communications (NFC), accelerometer, etc. All of these sensors are designed to share data freely, and your phone is constantly communicating all kinds of data to the outside world, through these radios and sensors.

I even showed you a simple demonstration of this data-sharing in the first chapter, remember?

By simply making you visit a webpage, I was able to determine a bunch of things about you and your phones, such as your location, IP address, saved networks, and more.

Sure, there are legitimate instances where sharing this information is useful and/or necessary.

For instance, you might want to share your location with someone when you are planning to meet with them. Or you might want to orient yourself when you land in a new city. Or you might want to evaluate your network to see if there is any vulnerability.

However, each of these situations demands active participation and consent. Therefore, the simplest (and the best) course of action would be to switch on these sensors only when required and switch them off as soon as you are done. The details on how to achieve this are provided under the #RohitRecommends section at the end of this chapter.

Permissions

In most cases, apps on your Android device cannot automatically access any sensor data just because they are installed on your device -- they need to be given explicit permission. Apps will request this by presenting you with a small dialog box [5] that says, Allow [XYZ app] to access this device's location? when you open the app.

Not all permissions need to be explicitly granted, however. According to the documentation available on developer.android.com:

The purpose of permission is to protect the privacy of an Android user. Android apps must request permission to access sensitive user data (such as contacts and SMS), as well as certain system features (such as camera and internet). Depending on the feature, the system might grant the permission automatically or might prompt the user to approve the request.

This differentiation in permissions (called Protection Levels in the official Android documentation) was introduced from Android version 8.1 Oreo. There are three protection levels that affect third-party apps - normal, signature, and dangerous permissions:

Normal permissions are those that are required when the app needs to access data outside its own sandbox, but the data that it is trying to access doesn't risk the user's privacy, for example, permission to access the user's time-zone.

Signature permissions are those that are given to certain system-critical apps included on the device by the manufacturer and typically grant access to certain system-level actions. At times, these apps cannot be uninstalled or disabled by the user.

Dangerous permissions are those that are likely to affect the user's privacy or the operation of other apps. The user is prompted to give permission to the app explicitly and the app cannot provide the underlying functionality until the user has explicitly approved the permission request.

.

For example, in the example above involving the GPS/location sensor and the XYZ app, if the user denies the GPS/location permission to the app, the app will not be able to display the user's current location on the screen.

I've detailed these permissions in the last chapter of this book, under a heading titled, " The 10 Android permissions listed under 'dangerous' protection-level", in case you are interested in knowing what these dangerous permissions are, and how they affect the privacy of your personal data.

macOS

Over the last few years, Apple has consistently held a market share of about 9-10% in the Desktop OS market segment, i.e. one out of every ten desktops is running the macOS operating system. However, in spite of having such a huge lead over Apple, Microsoft's overall market capitalization was still reported to be less than that of Apple. In other words, Apple earned more out of its meagre 10% market share than Windows did with nearly 75% market share.

Sure, it can be argued that Apple sells its products at a premium, a much higher cost than Microsoft does, and that certainly explains its massive market capital. However, it can also be argued that they have consistently delivered products that are worthy of the premium pricing model they employ -- both in terms of usability and stability. Moreover, Apple consistently claims their products are designed keeping the user's privacy in mind and, to some extent; they have consistently delivered on this promise as well.

Furthermore, the fragmentation present in Windows versions is very rarely seen in Apple devices. As of October 2019, approximately 83% of all devices running macOS run version 10.13, 10.14, or 10.15 - the three latest updates. In comparison, only 50% of Windows machines run Windows 10, while 40% still run Windows 7 [1] .

Hardcore Mac enthusiasts claim that MacOS offers the perfect middle ground between Windows and Linux, that is, it is as easy to setup and use as Windows while being as developer-friendly as Linux due to its Unix-based origins. However, even though it is based on FreeBSD [2] , macOS is proprietary software.

You might also hear arguments from people, claiming that Macs are better than Windows because they don't get viruses [3] or that Windows is better than Macs because you don't need to use proprietary hardware all the time . The internet is filled with tons of arguments of why one is better than the other, but I'm going to bow out of that conversation here respectfully.

All I am going to say about the Mac vs Windows debate is that neither of them is truly secure nor do they truly respect the privacy of the user -- well, at least as much as most of the Linux-based operating systems do, anyway.

Info

Apple's Stance on User Privacy

As an operating system, Apple is a lot more considerate about user privacy as compared to Microsoft and Windows – at least, by their own description. On their privacy policy page, Apple claims that they can create personalized experiences without using personal information.

RohitRecommends

Almost all of the current Android phone manufacturers have a significant vested interest in learning about your phone usage patterns. Getting to know how the average user uses their phone allows them to design the user experience in a way that enhances the utility of their phones for the user.

On the surface, this might seem benign, but the potential for misuse of this data is huge. At the very least, this dataset is ripe for targeted advertising. Therefore, it is in every user's interest to ensure that Google and other manufacturers get their hands on as little data as possible.

In other words, they claim that the data they collect is mostly processed on your device itself. Apple may still send some usage data to their servers in some cases, the details of which can be found in their Privacy Policy. The data that does get sent back to Apple servers are scrubbed, anonymized with rotating identifiers, and only sent to Apple servers after you give explicit permission to do so.

[QR Code: https://www.apple.com/privacy/approach-to-privacy/]

The thing is, different apps and features on your macOS device will have different ways of treating your data. Scanning the QR code given alongside (in this section) will take you to a page on the Apple website titled Our Approach to Privacy where Apple has described -- in a lot of detail -- the various ways in which they try and safeguard the privacy of the data contributed by Apple users.

Google Telemetry

It is extremely important to be aware of what data you and your device may be shared with various entities. To get an idea about what your device is sharing with Google, you can check the My Activity section in your Google account.

Open the Google Settings app on your Android device. If you don't see a Google Settings app, open the Settings app and click the Google section to open it. Click on Google account at the top to open your account page. Open the Data & Personalization tab and click the link titled, Manage your activity controls at the bottom of the Activity Controls section:

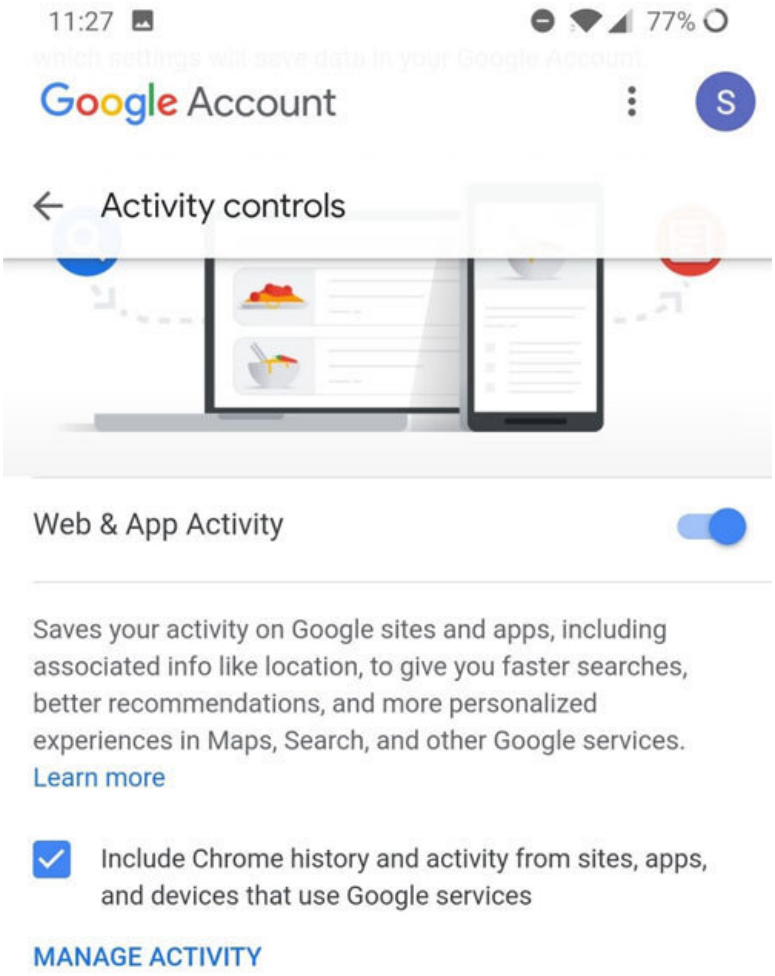


Figure 3.1: The "Activity Controls" section in a Google account accessed using an Android phone.

Alternatively, you can open your My Activity page in your Google account by going to:

https://myaccount.google.com/myactivity

Or, you can scan the QR code given alongside this paragraph and open; you're My Activity page using the browser app on your phone. Note that you may need to sign into your Google account before you can access this page in your browser.

Linux

This may sound strange to you, but Linux isn't an OS by itself. The term Linux is often used to refer to a family of open-source operating systems based on the Linux kernel.

The first version of Linux was developed by a 21-yr old Finnish Computer Science student named Linus Torvalds as a personal project to create a free operating system to use on his new PC with an 80386 processor. From there, the Linux project grew, and eventually collected a dedicated community of various kinds of Linux enthusiasts.

You'll often hear the words distribution or flavor in conjunction with the Linux family of operating systems. A distribution (or flavour) of Linux refers to an operating system made by combining the Linux kernel with additional utilities (for example, GNU tools, X Window System, Desktop Environment) and assorted software (for example, package managers and other software) in a manner such as to meet the needs of the user.

Info

GNU's Not Linux!!

Notice that I used the phrase, 'a Linux-based operating system' This is because, contrary to popular opinion, Linux is technically not an operating system. It is the 'kernel' of the operating system.

In simpler terms, if I could draw an analogy to a restaurant, the kernel would (probably) be the restaurant manager who delegates work to the kitchen staff. The kitchen would be the system hardware, the various staff would be the 'drivers', and the entire restaurant setup would (probably) qualify as the shell .

More than six hundred such Linux distributions (or distros , as they are popularly called) exist today, and at least five hundred of them are under active development. These Linux distros can be either commercially-backed (for example, Fedora, openSUSE, Ubuntu, and many more) or entirely community-driven (for example, Debian, Gentoo, Arch Linux, and many more) and can be installed on a wide variety of devices such as servers, desktops, laptops, phones, tablets, and more.

One of the biggest advantages of having so many distributions is that you can choose a distribution that best fits your needs. Looking for something similar to macOS? There's ElementaryOS. Looking for something simple? Try Ubuntu. Are you looking for something lightweight? Maybe Lubuntu, Xubuntu, or Puppy Linux is more up your alley. Are you looking for something secure-ish? Well, you can try Qubes, TAILS, or similar distribution. There's a flavour of Linux for everyone.

That said, one of the biggest arguments against Linux is the unavailability of various tools and software that we take for granted on Windows, the biggest example of them being Microsoft Office. Instead, most Linux users rely on alternatives such as Libre Office, WPS Office, or web-based alternatives such as Google, and Microsoft Office Online to work with Office documents on Linux.

Note

As of July 2019, no official Microsoft Office installation is available for Linux, although you can still use the (somewhat limited) Office 365 version on your Linux machines. There are workarounds that allow you to run Microsoft Office on Linux machines, but none of them is officially recommended by either Microsoft or The Linux Foundation.

Lastly, while the newer versions of Linux are quite user-friendly, I must warn you that it has a different operating philosophy as compared to the other operating systems in the market. As a result, people switching to Linux often feel overwhelmed and may feel the need to immediately switch back to whatever OS they feel comfortable with.

However, in my opinion, once you get past the steep learning curve, you will soon realize that Linux is one of the most powerful, most secure, and most customizable operating systems you will ever use. This further evidenced by the fact that Linux is a major player in almost everything except the Desktop OS market. For example, the biggest companies use Linux-based servers, the fastest supercomputers run on Linux, and one of the most popular mobile operating systems, Android, is basically a port of Linux.

Multi-OS systems

All of the common configurations that we have seen so far have all involved computers with a single operating system, that is, the computers were configured to run one of the three available OSes, viz. Windows, or macOS, or Linux. However, it is possible to run multiple operating systems on the same computer without having one clash or corrupt the other. These configurations are commonly referred to as multi-OS systems and are only used in rare-but-specific scenarios.

We'll first take a look at the various multi-OS configurations and then evaluate potential scenarios for using multi-OS setups.

BASIC: (1 point)

Each section describes the data that is being shared by your device with Google at any given point in time. Toggling any (or all) of the switches in the right to OFF will change the quality and amount of personalization that Google can provide -- sometimes even significantly -- thereby impacting your usage experience.

Click on the Learn More link in each of the sections to get a better idea of what data Google stores about you.

Next, disable as much of Google's tracking activity as possible, that is, toggle only those switches on that you absolutely cannot do without, to the OFF position.

Google will still maintain some anonymized info about you but toggling these switches will at least limit the amount of information they will be able to use.

Dual boot

The most common multi-OS scenario is what is commonly known as dual-booting. It involves partitioning the computer hard-drive into two or more partitions and installing different operating systems on each partition. A special software tool called the unified bootloader is assigned the task of reading the various partitions and listing the various operating systems available on each partition.

In dual-booted (or triple-booted, or multiple-booted) systems, the user *must* choose the OS to boot into. Each operating system operates independent of the other, and all hardware resources are available for the operating system that is chosen at boot. To boot into another OS, the active OS needs to be shut down, and the machine needs to be restarted.

Typically, the 'dual-booting' setup is most commonly employed by users who are comfortable at working with multiple operating systems. Machines with Windows/Linux or MacOS/Windows (a.k.a. Hackintosh?) are the most commonly found dual-boot options.

INTERMEDIATE: (2 points)

There's still the matter of the data that Google has already collected about you. You also know that Google has already collected vast amounts of historical location data, web search and app usage data, device information, voice and audio activity, and even your YouTube watch history!

You can see all the data collected and stored by Google by going to:

https://myactivity.google.com/myactivity

Virtual machines

A virtual machine (popularly called a VM) is an emulation of a computer system running on another computer system, that is, a VM is a computer - called a guest - running inside another computer - called the host . Both computers share the same hardware resources, that is, the same processor, the same graphics card, the same storage, the same memory, and many more.]

The advantage of using VMs is the availability of multiple configurations on one single machine, that is, you can have multiple guests running many different distributions of Linux, all on the same host – though, not necessarily at the same time. However, since VM access the hardware indirectly through the host, they can often be inefficient and sometimes hinder the performance of the host system.

That said, for users looking to try out Linux, I highly recommend installing the latest version of a popular Linux distro (for example, Ubuntu, Mint, or Elementary OS) in a VM on an operating system you are already familiar with, such as Windows or macOS. The internet is full of multiple step-by-step guides, videos, and tutorials that will help you do this on your PC or laptop.

Alternatively, scan the QR code shown alongside this paragraph and open the My Activity section of your Google account, using the browser app on your phone.

Live OS

A Live OS is an entire, functional operating system that can be booted off a detachable storage volume, that is, a USB, a DVD-ROM, or a CD-ROM. While the latter two options (viz. a DVD-ROM and a CD-ROM) are not used as frequently in this day and age, I have mentioned them here as they constituted the first iteration in this concept. Many operating systems including macOS, Windows, and multiple Linux distros can be made

available as Live USB.

Lightweight operating systems, installed on bootable media (such as CD and DVD-ROM drives) and equipped with command-line interfaces, were initially used by technicians and computer enthusiasts to repair booting issues on computers. These soon gave way to Live USBs with the introduction of USB booting in personal computers in the early 2000s. These live USBs were superior to their CD and DVD counterparts due to the ability to read AND write the data stored with the OS. Moreover, since moving parts are absent in USBs, it allowed for faster read times, thus ensuring that a live OS on a USB could be booted fairly quickly as compared to a Live CD.

These days, most live operating systems allow for full read and write access, meaning you can make persistent changes to the operating system. These changes can be made to the bootable USB itself or can be written to the persistent storage on the computer's hard-drive. As a result, most live operating systems available today can be classified into two major types -- persistent and ephemeral.

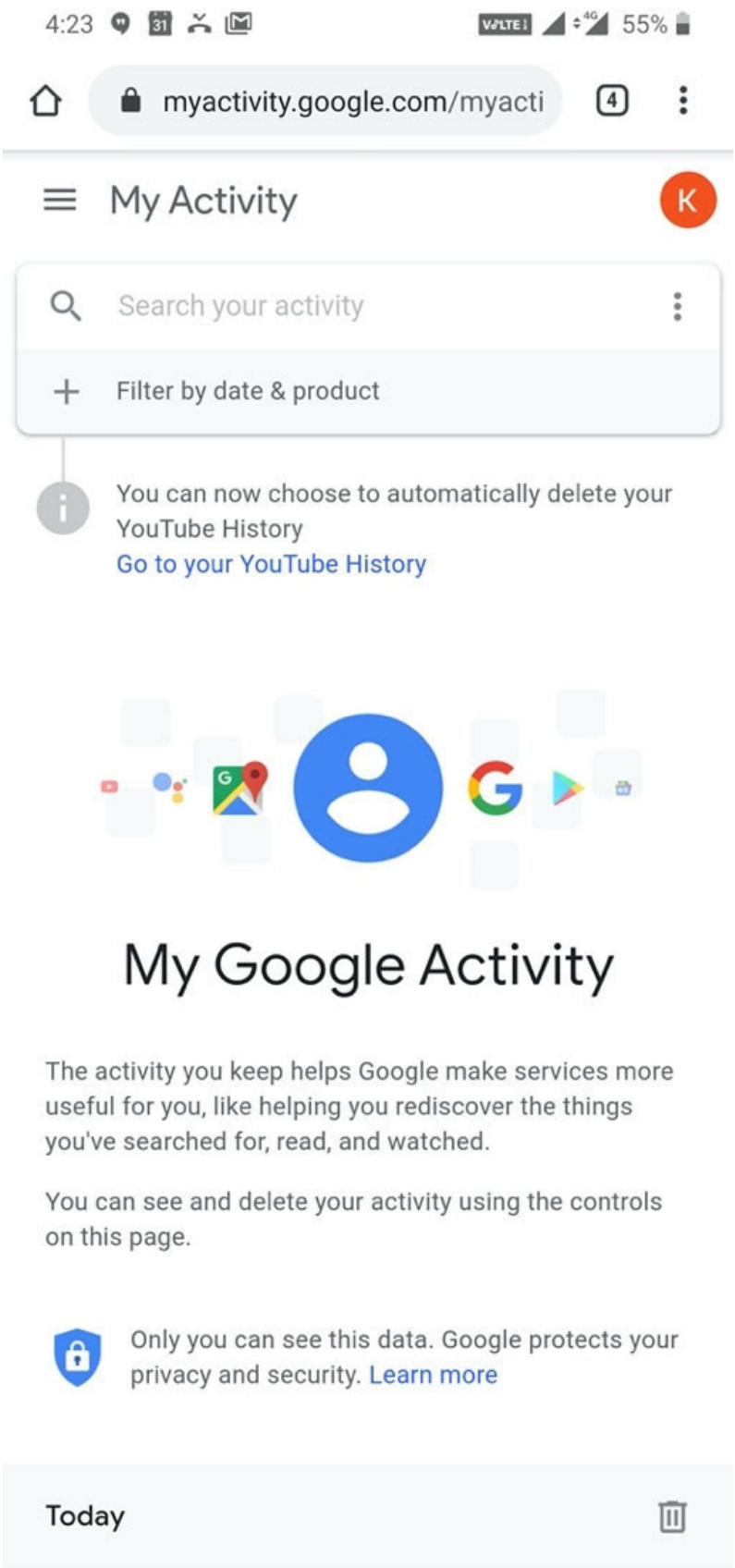


Figure 3.2: The "My Activity" section in a Google account accessed using an Android phone.

Click the link that says Delete Activity by , then under the Delete by date section, select All time in the dropdown, and click Delete . Read the confirmation dialog that appears, and then click on Delete again.

Click on the link that says Other Google Activity and, one-by-one, choose which activities you want to delete and delete them. Scroll down to the section titled Other Activity .

Choosing to follow this recommendation means that your internet experience will change -- somewhat or significantly – depending on which of the switches you toggled OFF . For instance, you might find that switching the Web & App Activity to off and deleting your activity data will result in severely limiting the functionality of Google Assistant.

Note that this does not delete the data from Google's servers; it merely prevents Google from using it to personalize your experience .

Data persistence

Some live USBs allow you to make changes to the live operating system, and these changes are persisted across reboots. For instance, while running the Live OS, if you were to install specific software or download a specific document or file to the system, that software, or document, or file can be made available each time the system reboots.

Data persistence can be limited or full-install, that is, you can choose only to persist data across sessions (either on the USB or local storage) or you can choose to install the full operating system on the USB. Although installing the entire OS on the USB ensures greater security and faster boot times, it must be noted that not all operating systems allow for full installations on the USB. Moreover, installing the entire OS on a USB requires a significant amount of storage space to ensure that both the OS and user data can be accommodated.

For most use-cases, using a Live OS with data persistence across sessions is a great way to test-drive various Linux distros before fully installing them on your computer. However, this data is usually left unencrypted, so there is some amount of risk involved if you happen to lose the physical USB drive.

Leave No Trace

In contrast, you can choose to NOT persist any data across reboots. Each reboot of such a live OS results in a version of the operating system identical to the one that was booted during first-run. These operating systems run solely in the available RAM and do not write anything to the host storage system. As a result, they leave no trace of their existence and are also called amnesiac operating systems.

Such amnesiac live operating systems come in very handy whenever you use any machine/s in a semi-private or public setting/s that you do not trust, for example, your neighbor's computer, or computers at cyber cafes, exhibitions, public libraries, and many more. Since the Live OS operates only within the confines of the memory, no data is written to the host system's hard disk, that is, it leaves no trace on the host system.

I therefore strongly recommend that you always carry a bootable USB with an amnesiac Live OS (such as Tails, Subgraph, or Qubes OS) in case you have to use an unknown computer in a semi-private or public setting. This will ensure that you do not accidentally share any data on unknown machines and will provide you with a familiar and secure OS environment to work with.

ADVANCED: (3 points)

For the more advanced users, I'd recommend blocking telemetry information from being sent out from your device. The two methods described below are merely popular examples; a little research on the internet will yield various other options that might prove suitable for your own unique situation.

Consider installing a more powerful adblocker like AdAway or Blokada on your phone. Both AdAway and Blokada rely on lists of known ad-servers and block all requests made to them. While Blokada accomplishes this by installing a 'local' VPN on your device, AdAway downloads the lists as a host file and, therefore, requires root.

Root your phone, and install a device-appropriate custom ROM that is known to be privacy-aware, such as Lineage OS, Una OS, or Replicant. A quick search on the XDA forums will reveal other options suitable for your Android device.

Default user: administrator vs guest

One of the biggest security mistakes (usually on Windows systems) that most users make is using their operating systems under the default administrator account, and often without a secure password. This is highly risky since anyone with physical access to the system can log in and install malicious software (such as keyloggers, Trojans, and many more) without the owner's knowledge or permission.

Typically, most operating systems recognize three classes of users:

Administrators: These are accounts with elevated privileges, that is, controls all the critical administrative functions such as installing and removing programs, adding and removing users, device maintenance, adding and removing restrictions, and many more. Basically, these accounts have the privilege to do anything and everything that has the potential to affect system performance. These are called administrator accounts in Windows, and root on macOS and Linux systems.

Standard users: These are standard accounts that can access most functions of the computer (such as running various programs), but they aren't allowed to make any significant changes (installing programs, adding/removing users, and such) to the system. Windows refers to these as

standard accounts, while macOS and Linux refer to them as simply user accounts.

Guest: A Guest account is (usually) a password-less account, available only on Windows and macOS systems. Any user can log in to the computer as a Guest and access various programs on the system. In Windows systems, any downloads, documents, files, etc. created or saved under a Guest account will persist across sessions, whereas on Apple systems, everything created during a Guest session is deleted after the user logs out.

Only Linux insists on creating standard accounts for users during OS installation. For both Windows and Apple systems, it appears as a recommended step, but it is not mandatory to create a non-administrative user during installations. The primary user of both macOS and Windows systems is, by default, an administrator account by default. Therefore, I strongly recommend that you create a separate, standard user for daily use -- either during installation or when you log in for the first time.

Both macOS [4] and Linux allow for further control over user accounts through the use of user groups. You can define various user groups and give each user group specific access to your system. For instance, you can define a group that only has access to certain devices, for example, a printer, to ensure that the printer is not overused.

EXPERT: (5 points)

At this level, you might be required to invest some significant resources -- in terms of both money and time -- to ensure the privacy of your personal data:

If you must use an Android phone, do seriously consider switching to more privacy-aware alternatives, such as the SilentCircle BlackPhone2 and UnaOS. The Apple iPhone is also a viable option that is certainly worth considering.

It is possible to use Android without installing *any* Google services. However, this requires a significant amount of technical expertise and know-how and we absolutely, positively, comprehensively recommend that you DO NOT do this on your own. We strongly recommend consulting with experts if you want to set up and use your Android phone without Google services.

Important!!

Message From My Lawyer: If you still want to give it a shot, refer to Chapter 15: Set up your Android WITHOUT Google services. Once again, I do NOT recommend doing this without expert consultation. Should you decide to proceed, you will be doing so at your own risk, and neither the publisher of this book nor I shall be held liable should anything go wrong during the process. For once, I agree with him (my lawyer, that is) whole-heartedly!

Telemetry

Telemetry refers to the automated collection and remote monitoring of data and measurements from a device, or devices. The data collected through telemetry is typically used to understand various kinds of patterns created in the process of using the device. Typically, for operating systems, telemetry may be used to understand how various features get used, or diagnose errors arising out of device usage, or measure performance and other related metrics.

A lot of times, when I (or other privacy and security experts) say that your devices are sharing data without your consent, I (or we) are usually referring to telemetry. My issue with telemetry is that the data collected through even the most basic telemetry exercise can be easily leveraged and manipulated to create profiles of individual users, which is rather detrimental to user privacy [5] .

Let's look at the telemetry behaviors of various operating systems, shall we?

Non-Google Telemetry

As I said earlier, Google isn't the only company that has access to your device and is interested in your data -- your device manufacturer is looking for ways to get a hold of that data too!

If you've followed either of the two recommendations under ADVANCED , then you are already set - nothing to do here. If you haven't or are looking for alternative recommendations, then I suggest you follow the recommendations listed below.

Windows 10 telemetry

One of the biggest arguments against Windows 10 that you'll hear from various privacy advocates is the automatic data collection spread across various features of Windows 10. Many privacy experts have even gone so far as to call it a privacy nightmare because of the amount of data it collects from its users.

Right from the moment it boots up for the first time, Windows 10 constantly sends back data collected through various user interactions to Microsoft servers. Every time you search for something on your PC, or connect to a Wi-Fi network, or update your OS, you voluntarily share your

data with Microsoft servers, which is then used to improve your Windows experience .

BASIC: (1 point)

If you don't own a device that runs stock Android, then I strongly recommend following these recommendations to opt-out of intrusive telemetry and unwanted advertising by various manufacturers - specifically OnePlus and Xiaomi.

OnePlus: To opt-out of the OnePlus device User Experience Program , open the Settings app, scroll down to System . You'll find multiple checkboxes under Experience improvement programs that you can toggle OFF right away.

Xiaomi: Someone over at XDA forumswrote a great post titled, Ads in MIUI 10 hamper the experience on otherwise great hardware: Here's how to fix them. It does a pretty good job of detailing how to get rid of recommended apps and ads on most Xiaomi smartphones. You can read it here: https://www.xda-developers.com/xiaomi-miui-ads-hamper-user-experience/

Scan the QR code given alongside this paragraph to read the post on your phone.

Diagnostics and feedback

No matter how much you restrict them, Microsoft still collects what they call basic diagnostic data, which they define as follows:

Basic diagnostic data is information about your device, its settings and capabilities, and whether it is performing properly. This is the minimum level of diagnostic data needed to help keep your device reliable, secure, and operating normally.

You can see this for yourself in the Windows 10 Settings application. Click on the Start menu, then click on the Settings gear icon, and click on Privacy . Then, click on the Diagnostics & Feedback section in the sidebar on the left.

Others: For most phones, the telemetry options can usually be found in the Settings app under the section titled System or whatever is the appropriate equivalent for your device. If you don't find it in your phone, then either your phone doesn't have a telemetry program or doesn't advertise its telemetry.

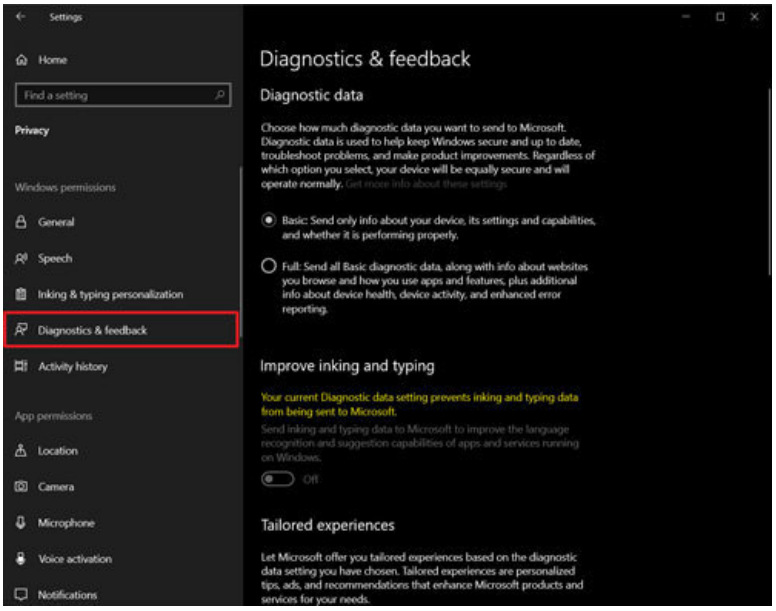


Figure 7.1: Screenshot of the Diagnostics & Feedback section under Settings > Privacy in Windows 10 (v1903)

What's even more worrying is the description under the second option, named Full because this is theoption that is enabled by default. Under full diagnostic data , Microsoft collects a comprehensive amount of data about your system and your actions on the system, which it describes as follows:

Full diagnostic data includes all data collected with Basic, along with information about the websites you browse, how you use apps and features, plus additional information about device health, device activity (sometimes referred to as usage), and enhanced error reporting. At Full, Microsoft also collectsthe memory state of your device when a system or app crash occurs (which may unintentionally include parts of a file you were using when a problem occurred). While your device will be just as secure and operate normally, if you choose the Basic level of diagnostics, the additional information we collect at Full makes it easier for us to identify and fix issues and make product improvements that benefit all Windows customers.

If you want to see what data is being collected exactly, scroll down, toggle the section titled View diagnostic data on, and click on the button underneath named Open Diagnostic Data Viewer to download the eponymous tool from the Microsoft Store. Install the tool and wait for a few days for it to collect the data.

Sensors

In Android, toggles for various sensors are almost always available via the Notifications drop-down. Note that switching off the sensors means that manual intervention will be needed at a later time.

For instance, turning off the GPS/Location sensor also means that Find my Phone service on your Android will not work as effectively since it can't accurately locate your phone. Apps that rely on location data (such as Maps, Uber, Ola, and more.) won't work until you turn the GPS/Location sensor on.

Similarly, you will need to manually turn on the Bluetooth sensor to connect to your car stereo or your Bluetooth speaker at home. You will need to toggle your Wi-Fi and mobile data when you move in and out of range and so on.

BASIC: (1 point)

Here's a quick guide on how to disable the various sensors on your device:

Swipe down to pull the Notifications screen. Swipe down again to expand the row into a grid:

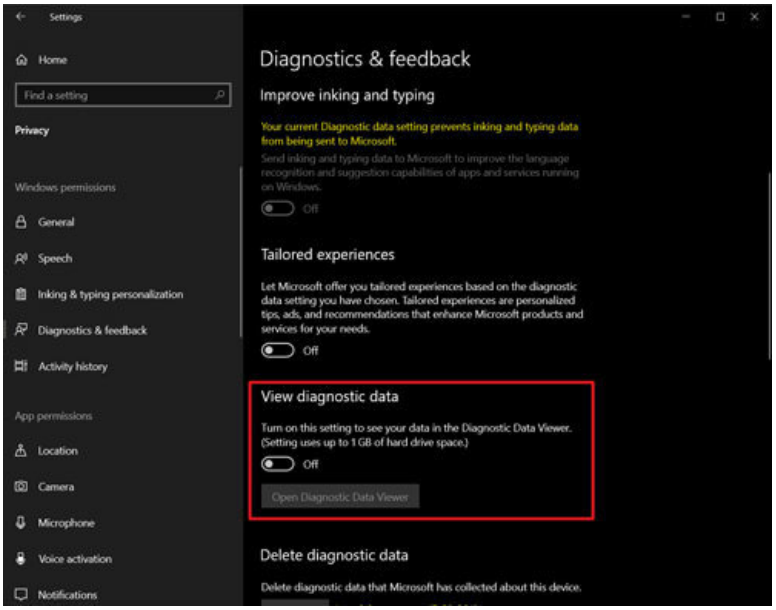


Figure 7.2: The option to turn on Diagnostic Data viewing capabilities in the Diagnostics & feedback section under Settings > Privacy in Windows 10 (v1903)

Note that this will collect and store any diagnostics data collected (upto 1 GB or 30 days, whichever is less) on your PC.

Keystroke logging

In January 2015, Microsoft announced the availability of an assistant feature named Cortana for Windows 10 desktops and mobile devices. Cortana is an intelligent assistant (similar to Siri and Google Assistant) who learns your behaviors and tailors recommendations and suggestions to match your day-to-day usage and behavior. For this to be made possible, however, Microsoft needs to collect all kinds of data, including but not limited to speech, inking, and typing.

In other words, everything you type, say or draw on a Windows 10 device is available for Microsoft to acquire and analyze. While some may see this as a necessary 'sacrifice' to improve the operating system's capabilities by way of personalization, I see it as excessive sharing of data with

Microsoft.

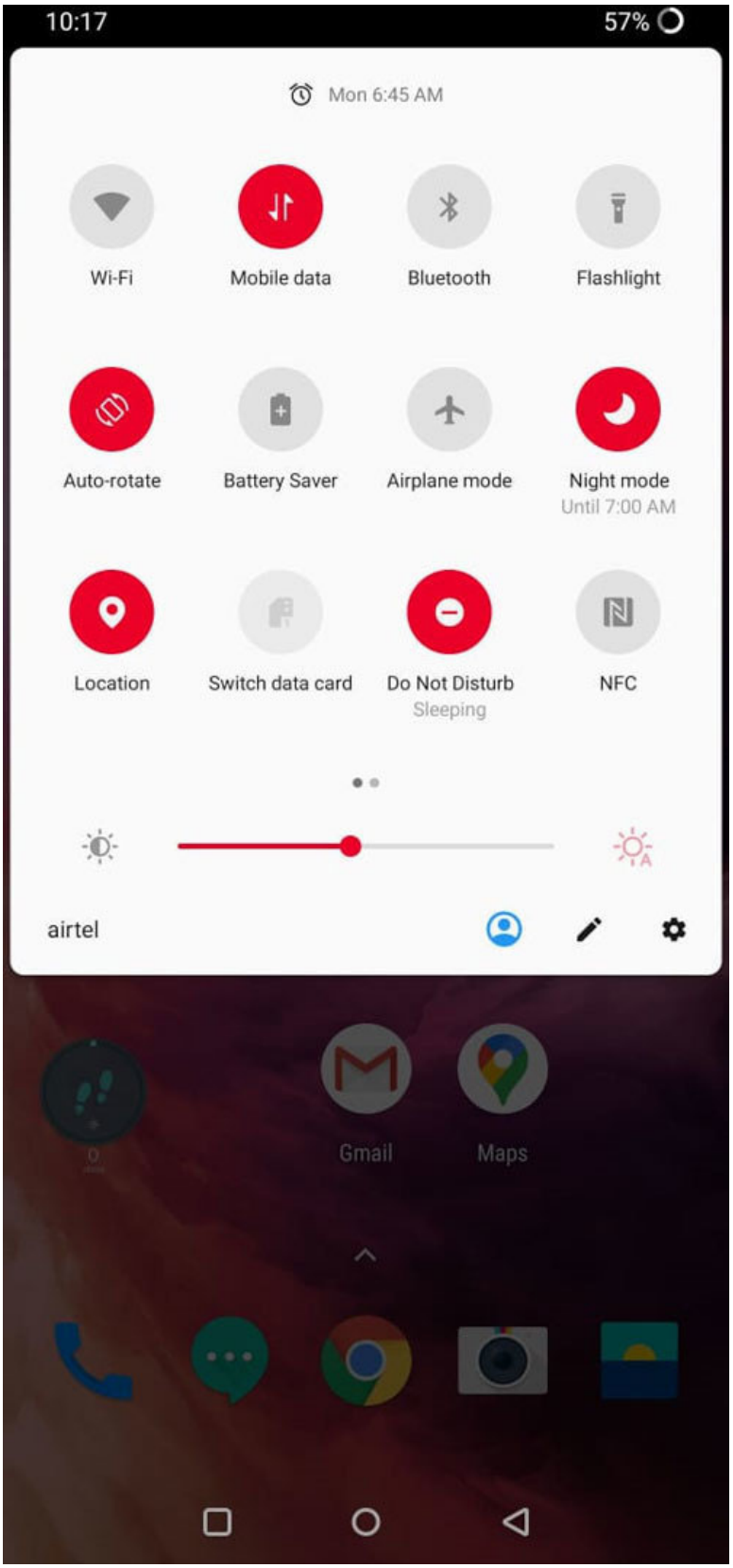


Figure 3.3: Accessing the notifications screen on a typical Android phone.

Locate the various icons for different sensors present in your device. Alternatively, open the Settings app on your phone.

Switch on only one of Wi-Fi or Mobile Data -- keep the other switched off.

Keep all the other sensors - GPS, Bluetooth, and NFC - switched off. If you don't see the GPS sensor toggle switch, look for an icon named

Location instead.

Hint

If you don’t see all sensors, look for a small pencil icon that allows you to edit the icons in the notification grid. Perform the necessary actions to make these icons ‘active’ and bring up the Notification grid again.

Since these sensors consume quite a bit of battery, as an added bonus, switching off these sensors will help prolong your battery life as well!

Cortana

Cortana, who derives her name from the famous Halo franchise of games on Xbox, is the name of the digital assistant introduced by Microsoft in January 2015. Since then, Cortana has been integrated into numerous Microsoft's products, such as Microsoft Edge browser, Bing search engine, Band smartwatch, and more.

Info

For people who have installed (or upgraded to) Windows 10 version 1903 or later, Cortana and Search have been split into two separate sections. Cortana and Search both now have their own sections in the Settings screen. I would strongly recommend checking out the various privacy options under each section and toggling any switches that are designed to share your data with unwanted third-parties.

Cortana provides you with a plethora of personalization options through something called the Notebook . To access Cortana's Notebook, open the Cortana app, click on the hamburger menu (that is, the three horizontal lines at the top left) and click the Notebook icon below the Home icon.

Permissions

Starting with Android 6.0 Marshmallow, Google introduced the runtime permissions model for users to manage the permissions being given to various apps directly at runtime. What this means is, regardless of what permissions the app asks for during install, the dangerous protection-level permissions will be explicitly requested from the user by the app when the app is opened.

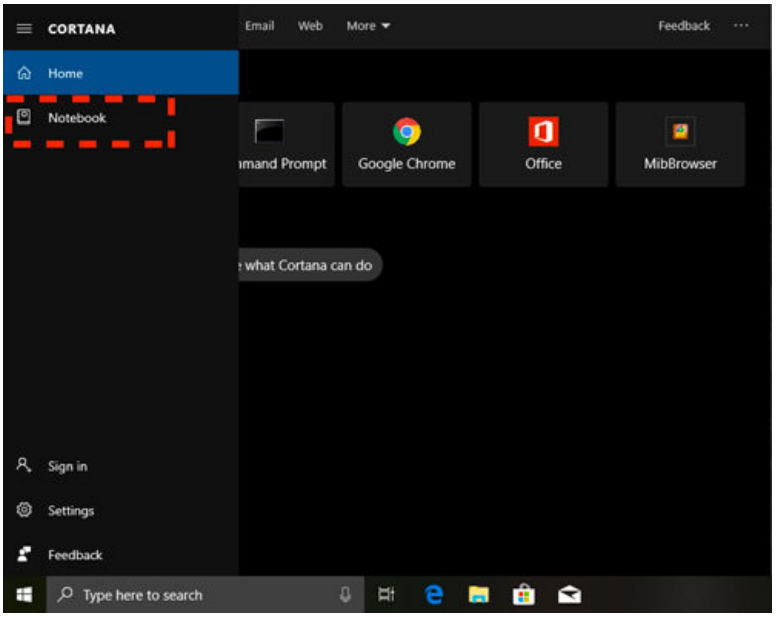


Figure 7.3: Cortana's 'Notebook' can be accessed by clicking the 'hamburger' menu button on the top left.

Here you'll be able to see and edit various personal settings and interests which Cortana will use to personalize your Windows 10 experiences. You'll find that Cortana can acquire information about a wide range of things, starting from your name to the weather in your city, to more intrusive details such as contacts, calendars, and meetings on your schedule.

BASIC: (1 point)

I've already explained how the various app permissions available for Android apps affect your privacy. The minimum you should do knows the different permissions that each one of your apps has been granted.

This is actually quite easy to do because Android provides a nice interface to view all your apps categorized by the permissions granted to them.

In your Settings app, click Apps & Notifications , and then click App Permissions or whatever is the equivalent [6] for your device. If you did it right,

you should be looking at something similar to the following screen:

Wi-Fi Sense

In a bid to help users connect with wireless networks easily, Microsoft provides a feature called Wi-Fi Sense in older versions of Windows, and this feature can be enabled by default, assuming you don't pay attention to it during Windows installations.

Wi-Fi Sense allowed you to connect automatically to trusted open Wi-Fi hotspots, that is,Wi-Fi hotspots that other Windows 10 users have connected to in the past. If any of these users happened to be a friend (that is, happened to be in your Skype, Outlook, or Facebook contact lists), then you could connect to all Wi-Fi hotspots that were previously connected to by this friend . Wi-Fi Sense was discontinued by Microsoft after it received tremendous backlash from security researchers for ignoring the obvious privacy implications inherent in its design.

Microsoft made this possible by encrypting your Wi-Fi password and storing it on Microsoft servers. I will not debate whether or not Microsoft's servers are secure enough for this action to be considered safe – that's another matter, for another book.

However, consider this scenario: Say, you enable Wi-Fi Sense on your Windows 10 machine. Say, a neighbor in your building happens to be your Facebook friend who also uses Windows 10 and has Wi-Fi Sense enabled on their machine. This means that your neighbor can connect to your Wi-Fi network and vice-versa! Since this applies to ALL your friends on Skype, Outlook, and Facebook, the obvious question is: do you completely trust ALL of your friends on Skype, Outlook, and Facebook? What happens if one of them happens to be an adversary?

The privacy nightmare doesn't end here. Say, you do the responsible, recommended thing and disable Wi-Fi Sense on your Windows 10 machine. At some point, a neighbor asks for your Wi-Fi password and connects with their Windows 10 device with Wi-Fi sense enabled and the 'Share network with my contacts' option enabled. Now all the people in your neighbor's Skype, Outlook, and Facebook contact lists have access to your password-protected Wi-Fi network, even though you explicitly denied Microsoft any access to it!

Forget the privacy and security considerations for a moment and answer just this: In this day and age, do you really want people to be able to access the internet through your Wi-Fi network without your explicit permission or knowledge?

Note

Wi-Fi Sense is Discontinued. NOT!

Although Wi-Fi Sense has been 'discontinued', the option to sync Wi-Fi credentials between machines sharing the same login account still exists. That means, if you log into a new Windows 10 machine using the same Microsoft credentials, then you can 'import' various settings from one machine to the other -- one of which happens to be the Wi-Fi passwords stored on existing machines. As for macOS, a good password manager such as LastPass, Bitwarden, or Keepass works much better than Keychain to manage your passwords.

Figure 3.4: The "Permissions" screen under the Apps section of the "Settings" app on your Androidphone.

Drill down into each of the permissions listed here and make a note of the various apps that have been granted this permission. The toggle switch next to each app indicates whether the app has been granted or denied specific permission:

Apple's Keychain and 'KeySteal'

Apple also provides a feature similar to Wi-Fi Sense as a part of macOS, called Keychain . Keychain is also available for iOS, that is, Apple iPhones.

Keychain is a macOS application that stores your important private information (such as usernames and passwords for the Safari browser, credit cards, Wi-Fi passwords) on approved devices connected with the same iCloud ID. The problems with the mac OS Keychain are the same as those of Wi-Fi Sense. Furthermore, obvious vulnerability notwithstanding, Keychain has also been shown to be vulnerable on multiple occasions by multiple researchers.

In 2017, an information security researcher tweeted an exploit for Keychain that could extract stored passwords in plaintext. This exploit was immediately patched by Apple in the macOS High Sierra 10.13 supplemental update. In February 2019, a German researcher discovered the KeySteal vulnerability in macOS Mojave 10.14 through a different exploit that could be used to extract all the data stored in the Keychain by installing a hidden malware. Apple patched this vulnerability in a subsequent update, but Keychain continues to remain a lucrative target for many more exploits in the future.

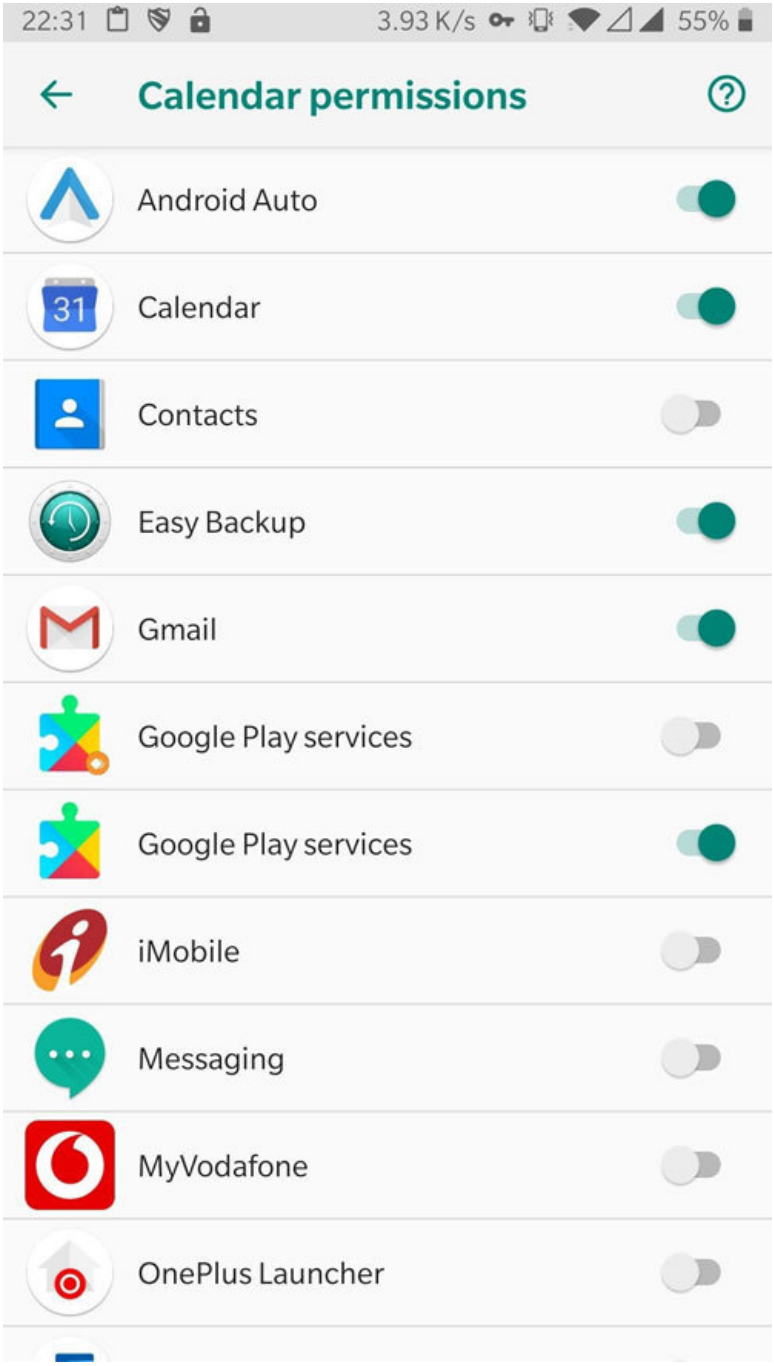


Figure 3.5: Drilling down into the Calendar permission in the "App permissions" screen.

Look for any apps that seem to have permissions inconsistent with their usage; for example, a Flashlight app shouldn't be given the Location permission. Refer to the Appendix (A) for a quick explanation for the various 'dangerous' permissions, if you wish.

Info

Importance of reviewing app permissions

If, at any point, you were wondering whether drilling down these permission groups was a waste of time, let me remind you what Facebook and Uber did a few years ago.

In 2016, Uber updated their app always to track the user's location, that is, collect location data in the background, from previously only collecting the data while the app was in use. In 2014, Uber was discovered to have implemented a real-time aerial tracking system called God View that used personal information to identify and track riders. In 2011, Facebook settled with the Federal Trade Commission and agreed to undergo an independent privacy evaluation every other year for 20 years over charges that it didn't keep its privacy promise to users by allowing private information to be made public without warning.

You might feel like you can trust behemoths like Facebook and Uber with your data, but these behemoths are as vulnerable to hacking attempts and data leaks as anyone else out there. For example, in 2013, Facebook disclosed details of a bug that exposed the personal details of six million accounts over approximately a year. Uber concealed a massive global breach of the personal information of 57 million customers and drivers in October 2016.

In a world where no one can guarantee the security of your data, wouldn't it be prudent to share as little data with anyone -- especially, these behemoths -- as possible?

Other privacy settings

As of July 2019, the latest update of Windows 10 (version 1903) still had a few data-sharing settings that could be construed as significant privacy concerns. Primary among these was the unique advertising ID allocated to each Windows 10 machine, at the time of installation. You can find this in the General section of the Privacy category in the Settings app, which can be found in the sidebar. There are a total of four major sections in the sidebar:

General

Speech, inking, and typing

Diagnostics and feedback

Activity History

In some cases, sharing this data can help personalize the various recommendations and suggestions you see on your Windows 10 device. However, from the perspective of minimizing data-sharing with third parties, I recommend that you toggle *all* the data-sharing switches to the OFF position for each of the sections. I also recommend that you ensure that any data stored by Windows 10 (whether on your device or in the cloud) is immediately cleared.

Scrolling down further you'll notice a section titled App Permissions under which are listed various hardware devices and services (for example, Location, Camera, Microphone, and many more) which collect your data and share with Microsoft servers when toggled on.

INTERMEDIATE: (2 points)

Now that you've checked out the various permissions that apps on your phone have been granted, it is time to toggle a few switches!

Using your discretion, toggle the switch next to each app under each permission category to grant or deny that permission to the app. Don't worry; in most cases, the app will simply ask you for that permission again the next time you open it -- just remember to deny it when that happens.

For core Android apps that absolutely need certain permissions, (for example, the Contacts permission for the Phone/Dialer app) Android will display a warning dialog to inform you that, if you deny this permission, basic features of your device may no longer function as intended. It is usually a good idea to avoid the Deny Anyway option, and press Cancel in such situations.

Info

Google Play Services & Permissions

As you drill down into each permission category, you'll realize that Google Play Services appears in each one of them. That's because Google Play Services acts as a service provider (kind of like a trust-broker) for other apps on your device.

Many apps access data for performing various functions. For instance, Maps and cab-aggregator apps like Uber and Ola need the GPS/location permission to carry out their functions. Instead of requesting this information directly from the sensors, apps may then choose to request this information from Google Play Services.

Google Play Services, therefore, requests all permissions so that it can aggregate all necessary data from your device and provide it to any apps that may ask for it.

If you choose to deny permissions to Google Play Services, all you're doing is essentially declaring that you do not want Google Play Services to be a centralized provider of this data to apps on your phone. You are essentially stating that you want each app to request specific permission and not rely on Google to provide them with that data.

Most popular apps are well-designed and are programmed to handle this transition gracefully. However, you might find that some apps will not function properly after you choose to Deny Anyway for Google Play Services. This is because the apps rely solely on Google Play Services to provide them with that data.

You may also find that this change is *not* instantaneous; instead, apps will complain (or sometimes even crash) the *next* time you try to open them. When that happens, you will have two options: You can either decide to continue using these apps, or try and find suitable replacements for them.

RohitRecommends

Almost all of my recommendations in this section will be aimed at Windows 10 users.

Why? Because there isn't much to recommend for either Apple or Linux users! Both these operating systems have rather robust (and a pretty straightforward) philosophy about maintaining the privacy of user data. Furthermore, both these operating systems provide simple and straightforward opt-out methods for users who do not wish to participate in sharing any telemetry data from their devices.

Conclusion

Looking at Google's huge presence on the internet, it would be silly to assume that you can escape being tracked by them. The most you can do is severely limit the information that Google can acquire about you. To do this, however, would require entirely giving up on many of Google's excellent services such as Android, Gmail, and Maps, to name just a few.

Now, to be fair, some really good alternatives to all of these services exist and can be found across the internet. For instance, you could flash your Android phone with Lineage OS, use Protonmail and OpenStreetMaps instead of the native Google apps. However, this would mean that you'd be losing out on the inter-operability of its services -- one of Google's biggest advantages, which also happens to be a huge pain-point for privacy-enthusiasts like us.

In other words, finding suitable alternatives that will help reduce your dependence on Google (and its varied offerings) is a long and painful process. It is likely that you won't be able to achieve it all in one day. It is also likely that you won't be able to achieve complete independence from Google and its offerings.

I suppose that's the beauty of it, though. Ultimately, YOU get to choose how much you want to reduce your Google footprint.

---

[1] Yes, yes, I know Windows phones aren’t sold anymore. Microsoft announced in January 2019 that support for Windows 10 Mobile would end on December 10, 2019.

[2] The Windows phone has a significantly smaller market-share as compared to these two behemoths of the phone OS market, so we won’t include them in discussions in this book. Windows phone enthusiasts are welcome to ask me their questions by emailing their questions at discuss@privacy.clinic

[3] There is a way to install Android OS on your phone without using any Google services. I’ve touched upon it briefly in a bonus chapter at the end of the book.

[4] I am not trying to target any manufacturer specifically here. I have simply provided these examples as a way to show how things can go massively wrong, regardless of how well-intentioned they seem.

[5] On Android versions before 6.0 Marshmallow, apps are granted the necessary permissions during installation itself. According to the Distribution Dashboard on android.com, that’s about 25% of all Android phones in the market, as of July 2019.

[6] The exact name of the section may differ from phone to phone but the word 'permissions' will be mentioned somewhere, for sure.

Operating system (OS)

The choice of your operating system will determine which of the recommendations you will need to follow from this section. Simply put, I have assumed the following to be true:

You are a Windows user. Given that almost 90% of Indians use some version of Windows as their operating system; this isn't a very far-fetched assumption.

You haven't really paid attention to what Windows does with your usage data.

You are running a clean install of the latest version [6] of Windows 10 OS.

Windows is known to collect data from its users aggressively. On the other hand, macOS (and Apple) have openly proclaimed, on multiple occasions that they always choose to put the user's privacy ahead of everything else.

Since most Linux distributions are open-source and (mostly) community-driven, collection of user data is actively discouraged. That said, Linux distributions that are developed by specific organizations such as Canonical or Endless may collect some kind of telemetry data, but they usually provide an easy and straightforward way to opt-out of such data collection as well.

Thus, the recommendations that I have made in the following section are primarily based on three main criteria:

Desire to switch

Ease of use

Ease of switch

My recommendations for an ideal operating system are primarily based on whether or not you are open to switching to a new operating system -- everything else follows from there. If you are open to switching, then I'll evaluate and recommend an alternative OS that is relatively easy to use for your specific use-case.

Chapter 4

Apple iPhones

Introduction

The first Apple iPhone was demonstrated to the world by a very proud Steve Jobs at Macworld 2007—a trade show dedicated to all things Apple since 1985. From the moment he first spoke about combining the iPod, the phone, and the internet into one single device, the audience was hooked, and, in that moment, the world had changed.

Since that memorable day in January 2007, Apple has sold altogether about 1.5 billion iPhones worldwide. Furthermore, Apple has consistently been among the top 3 vendors in terms of the number of smartphone units sold in the last 5 years. iPhone sales have consistently accounted for more than half of Apple's total global revenue year after year.

Apple's stock has greatly benefited from the popularity of the iPhone, growing from just under $2 in 2001 to over $200 in 2019—a massive growth of over 15,000% in 18 years!! Apple also became the first publicly traded American company to have a net worth of over $1 trillion, making Steve Jobs one of the richest people in the world, at the time.

Most of Apple's success can be ascribed to the following three factors:

Premium branding: Apple iPhones are typically sold at a much higher price than most Android phones available in the market, making the iPhone a premium product. Not only does it help Apple's bottom-line, it also provides a sense of elevated status for the customer, thus making the whole deal a win-win for both parties.

Usability and design: Apple iPhones are designed with the average user in mind. While great care is taken to make the product look sexy [1] , Apple also ensures that the product by itself is easy-to-use by making its core functions extremely intuitive in terms of user experience.

Leadership thru innovation: Apple has been known to introduce and/or adopt various innovations that have later become industry standards. For instance, touchscreen devices existed before the iPhone, but the iPhone was the first touchscreen device that was deemed easy-to-use due to the simple-but-elegant interface accompanying it, viz. iOS.

In the last chapter, we compared Android phones to custom-built cars, all running the same engine viz. AOSP, but different peripherals and livery. We explained that Google Pixel, in the context of this analogy, was the phone equivalent of a stock car.

The Apple iPhone, too, is the phone equivalent of a stock car– except that every part of this stock car is made [2] by the same manufacturer, viz. Apple. In this analogy, iOS is the engine, the apps arethe essential car parts, the handset is the chassis, and Apple designs and manufactures all of them under its own brand. Furthermore, since they have established themselves as a premium brand, Apple iPhones are usually available at a premium as compared to Android Phones.

In this chapter, I will attempt to answer the question: From a security and privacy perspective, is it worth [3] paying the premium to Apple for their iPhone and/or other mobile devices such as the iPad?

BASIC: (1 point)

Important!!

I do not recommend using any version of Windows older than Windows 10.

I'll say that again: I absolutely do NOT recommend using any version of Windows older than Windows 10.

That means anyone using a version of Windows that is not Windows 10 (such as Windows 7, Vista, XP, or lower) must upgrade immediately to Windows 10, preferably the latest update made available by Microsoft [7] . The support lifecycle for all other versions of Windows has either ended or will end soon. The wide variety of vulnerabilities that have since been discovered and distributed may render your computer susceptible to various penetrative attacks by adverse actors.

In other words, if you are still running an older version of Windows, you are very likely to get hacked and/or your data stolen, and there's not much I (or anyone) can do to help unless you choose to upgrade your OS to the latest available version of Windows 10.

If you feel you are comfortable with Windows as your primary operating system aren't looking to change, then I strongly recommend that you do the following, at the very least:

Upgrade your Windows to the latest version: As of the date this chapter was written, this happens to be Windows 10, build 1903. If you are using Windows 8, or 8.1, upgrade to Windows 10 as soon as you can. Windows 7 users had until January 14, 2020, to upgrade and I strongly recommend that you upgrade to Windows 10 and get used to the (somewhat) different interface and OS behavior.

Update all programs to their latest version: While Microsoft automatically pushes various updates and patches continuously to ensure that your Windows is protected from various vulnerabilities, it is your responsibility to ensure that you do the same for the various third-party software that is installed on your system. An attacker trying to steal your private information will often try and exploit known vulnerabilities in such software to gain unauthorized access to your system.

Encrypt your data: For users with newer machines, I strongly recommend using encryption software to encrypt files on your system. If you are running the Ultimate or Enterprise versions of Windows, you can use the built-in tool named BitLocker, or you can use third-party tools such as TrueCrypt or VeraCrypt to encrypt your system

Maintain multiple backups and redundancy of data: Not matter how careful you are; there is always a chance something goes wrong. To protect yourself from mishaps, always maintain multiple copies of your most important documents and files. I always recommend maintaining at least three copies – one master copy, one in an external drive, and one online. Keep all three copies constantly in sync so that you can get back up and running should something somehow go wrong with your master copy.

Follow the various recommendations given across the book: Windows is the OS of choice for many Indians, and it is a tough ask to move from something they have (probably) used for almost their entire life. So, if you insist on continuing to use Windows, ensure that you follow the various recommendations given across this book, specifically this chapter. You must pay special attention to the parts on OS Telemetry and Bloatware.

This is the absolute bare minimum I recommend for any Windows system.

The Apple Ecosystem

Apple's ecosystem is what people in the business describe as closed , that is, non-Apple employees do not get to see, much less modify, the hardware or the code that runs on these devices. Developers who wish to publish third-party apps on the iTunes store must pay Apple a license fee AND adhere to Apple's strict guidelines.

Being a closed ecosystem does have some advantages, though.

One, inherent weaknesses in such proprietary systems get automatically hidden along with everything else. This method, typically called 'security through obscurity', is useful in deterring malicious actors from breaching the system, since they can't know what weaknesses to look for. Two, a closed ecosystem can be well-regulated through rigorous checks and balances, due to its (relatively) small scope. All contributors to the system are clearly identified and any errors (or malicious activity) in the system can be quickly traced to the source.

However, closed ecosystems can still be vulnerable. The most common (and famous) example, in the case of Apple, is the concept of jailbreaking your iPhone, which I will discuss in greater detail a little later in the chapter.

INTERMEDIATE: (2 points)

If you have the resources (financial, mental, as well as time) to spare, I strongly recommend switching to a more secure and more privacy-aware operating system such as macOS and/or a Linux distribution that works for you. Both these operating systems are built on the promise of user-privacy and known to keep user interests front-and-center with each of their major updates.

I understand that switching to a Mac will be expensive while switching to Linux is sure to be time-consuming -- I absolutely don't recommend doing either on a lark. In fact, I recommend doing this only after you have thoroughly evaluated your privacy requirements and are absolutely sure that you can afford it -- financially, mentally, and only if you have ample time to spare.

iOS

Unlike Google and Android, all Apple iPhones run the same operating system—iOS. iOS is a proprietary Unix-like operating system that is specifically optimized for running on Apple iPhones.

iOS is one of the most uniformly updated operating systems in the smartphone market. As of August 2019, 88% of all iOS-based Apple devices (that is, iPhones and iPads) that are actively in use have the latest version of iOS, that is, iOS 12, installed on them (source: https://developer.apple.com/support/app-store/). If you also count iOS 11 in the mix, the number goes as high as 95% of all eligible devices!

Apple usually also ensures that a majority of its older devices are compatible with the newer versions of iOS. For instance, iOS 13 is available for device models iPhone 6s and later, while iOS 12 and 11 can be installed on device models iPhone 5s and upwards.

In other words, (almost) all Apple iOS devices will (almost always) have the same interface, although the underlying hardware powering them may be very different.

Info

Since almost all iPhones run the same version of iOS, they provide a consistent interface for users across different device models, both old and new.

However, it also means that 95% of all iPhones share the same attack surface – the iOS 12 and iOS 11 software code. Therefore, any vulnerability found in either of these two operating system versions affects (almost) every iPhone out there in the world.

This scenario becomes even more horrifying if you consider that there may be unknown vulnerabilities (commonly referred to as zero-day exploits) being actively exploited by malicious actors to conduct unauthorized breaches of data.

ADVANCED: (3 points)

For those who are paranoid about their privacy and security, I recommend doing one (or both) of the following things:

A combination of operating systems by running one inside the other using a VM. For instance, the most common example is to run a privacy-focused Linux distro such as Whonix as a VM on a suitable host system. Ideally, having a privacy-aware OS (that is, macOS or a suitable Linux distro) for a host is recommended.

Always carry a bootable Live USB of a privacy-aware OS , such as Tails, Discreete, and many more. In case you absolutely need to access the internet using a semi-private or public machine, use this bootable USB to boot into the Live OS and access your data securely.

Personally, I carry a bootable Live USB with Tails installed on it everywhere I go. It comes in very handy when I need to use unknown computers.

iCloud

Along with its devices, Apple offers the iCloud cloud computing and cloud storage service to all Apple users, estimated to be around 850 million users as of 2018.

Users can wirelessly backup all kinds of data such as documents, photos, and music to remote servers and sync them across various Apple devices signed into the same iCloud account using iTunes. The multitude of features offered by iCloud (For example, Collaboration, Sync, Backup and Restore, Family Sharing, and more), combined with multi-factor authentication, certainly make it an option worth considering.

I'd like to mention here that iCloud does not use end-to-end encryption but, in their privacy policy, they mention that they take precautions—including administrative, technical, and physical measures—to safeguard your personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction.

Info

In 2014, extremely private photos stored in the iCloud accounts of several celebrities were anonymously posted to the imageboard 4chan, and later spread to imgur and reddit.

It was initially believed that the hackers managed to gain access through vulnerabilities in some Apple services viz. Find My Phone and iCloud itself. Apple, however, denied any insecurity in iCloud itself and claimed that the celebrities were spear-phished, that is, their account credentials were acquired through a highly targeted attack by malicious actors pretending to be from Apple.

Regardless of who was actually at fault, the fact remains that the personal photos of a bunch of individuals were accessed by someone who wasn't authorized to access them. They were accessed from a secondary location, the credentials to which were acquired through illegitimate means.

EXPERT: (5 points)

The configurations described under the previous level (that is, Advanced) will ensure that you don't accidentally leak your own data in a semi-private or public setting.

However, for users who want their privacy to be maintained in all scenarios need configurations that are more secure and more private than this. There are multiple ways to achieve this, all of which are mostly custom configurations designed for specific use-cases. Each one of them involves designing a specific (somewhat-complex) configuration that is rather unique to the requirements postulated by the user.

Jailbreaking

To put it in the simplest terms, 'jailbreaking' an iPhone is similar to 'rooting' your Android phone, but the motivations and scope of these actions is very different. In both cases, you (somewhat illegitimately) gain complete control over your phones but both actions can also render your phone vulnerable to malicious actions.

The act of jailbreaking usually involves exploiting vulnerability—either in the operating system code, or within the device hardware—to gain privileges as an administrative account or 'root' on the device.

Jailbreaking has several advantages from the end-user perspective:

Third-party apps: Apps that are unavailable through the official App store can be installed on jailbroken devices. This may include apps that have been banned, removed, deleted, rejected, or generally censored by the official App store.

Tweaks: Several unofficial tweaks and customizations are made by third-party developers, which can drastically alter the interface of your iPhone.

Unlocking: Carrier-locked and region-locked iPhones can be unlocked and used with other carriers and in other regions.

Privacy: Control the uploading of telemetry and usage statistics to Apple servers.

However, from a security perspective, jailbreaking can introduce some serious vulnerabilities on your iPhone:

Piracy: The most common reason for jailbreaking iPhones is to circumvent the official App Store and install pirated apps.

Malware: Malicious actors often install malware and tracking software on jailbroken devices.

Worm: An insecure SSH service on jailbroken devices can allow an attacker to gain entry onto your device and compromise your device usage.

Info

In November 2009, an Australian student created the first iPhone worm called iKee based on this insecure SSH service exploit to raise awareness about security issues around jailbreaking.

The same month, the Finnish cybersecurity and privacy company F-Secure reported the discovery of a new malicious worm that compromised bank transactions on jailbroken iPhones in Netherlands.

In August 2015, a malware named KeyRaider was discovered that was believed to have stolen the login credentials of more than 2 lakh users, affecting only jailbroken devices. KeyRaider was said to have affected users who downloaded apps from the Cydia app repository.

Since users with jailbroken iPhones are more vulnerable than regular iPhone users, and more likely to install pirated apps, it is in Apple's interest to pro-actively patch any vulnerabilities that can be used to jailbreak iPhones. Therefore, Apple actively releases various software patches for iOS to close down any and all jail-break vulnerabilities that are found. This why most jailbreaking software end up disabling OTA updates to ensure that users don't accidentally install these patches released by Apple.

However, if there happens to be a bootroom exploit, that is, an exploit found in the hardware of the device, it cannot be patched, unless you upgrade to a newer handset with newer hardware that does not contain the exploit. For instance, in September 2019, a bootroom exploit called checkm8 [4] (pronounced: checkmate) was discovered that affected all iPhone models upto and including iPhone X.

Opinion

I'm not explicitly trying to say that jailbreaking is inherently evil or jailbreaking is chaotically good. In fact, I do not have an opinion either way on the matter.

Legally speaking, jailbreaking is a violation of Apple's ToS and you shouldn't do it. However, jailbreaking also forms a significant part of the Right to Repair movement, if you believe in that sort of thing.

At the end of the day, jailbreaking, like rooting, is a highly advanced and technical thing to do to our iPhone. All I'm saying is that it deserves to be done with the greatest respect and utmost care.

Spy vs spy!

In one specific case, I was asked by a client to design a configuration that would leave little to no trace of identifying data if it were to be accessed from a random public computer, such as the one available in a library. This was a client working with intelligence agencies and needed to ensure that their browsing habits would not accidentally give away details about themselves.

This case was particularly challenging because operating systems often keep track of the timestamps when plug-and-play devices are plugged in and/or removed. Without administrative privileges, it would be difficult to remove any record of this data stored by the host system. Couple that, with the general surveillance options available to their adversaries, it was imperative that the client could access computers and leave no trace behind.

We, therefore, settled on creating a bootable USB with a slightly customized version of the TAILS distro, with a few additional persistent software, viz. a secure VPN, a secure messaging app, a disk-encryption tool, among other things.

The client was advised to tunnel into the TOR service through a VPN to ensure double redundancy and was strictly told to avoid frivolous browsing and/or logging into any websites on the internet. Their email service was moved to a more secure option, and all file-uploads were routed to more secure file-drop servers. Any messaging with the necessary agencies was either ephemeral or carried out over messaging apps with 2048-bit end-to-end encryption.

Although the client was mostly a Windows user, they managed to understand the new environment quite easily and were able to adjust their digital behavior and ensure maximum privacy and security, using the detailed steps that I had outlined for them.

Apple and Privacy

The biggest difference that sets Apple apart from Google is the way they treat user data. While Android has been known to (rather aggressively) collect all kinds of data from its users, Apple has labelled itself a product company and strongly distanced itself from any and all data-collecting activities.

In fact, Apple CEO, Tim Cook, explicitly stated in a May 2019 interview with ABC that Apple "has no interest in collecting users' data" because that's not their product, as they are in the business of selling devices. "You are not our product," he said. "Our products are iPhones and iPads. We treasure your data. We wanna help you keep it private and keep it safe."

If you think that means Apple does not collect any data from its users, you'd be very, very mistaken.

Apple definitely collects quite a bit of usage data from all Apple devices, except they claim that they only collect usage data, and not data stored on the device. Furthermore, even the data they collect is anonymized, (mostly) opt-in, and only collected to help improve their services, under the Differential Privacy [5] policy.

Note

Apple's Differential Privacy Policy

Telemetry

If you are worried about the amount of telemetry data collected by Microsoft servers, then there is a solution to ease your worries. Thankfully, in most of these cases, Microsoft has provided an option to turn off the sharing of such data (for what it's worth) by toggling the appropriate switches in the OS settings -- all of them bundled under a single heading called Privacy .

Regardless of what you ultimately choose to do with the data that your Windows machine is sharing with Microsoft servers, you need to aware of the scope and extent of data being collected under the Diagnostics and Feedback section under Settings . For purposes of this section, award yourself 1 point.

Let's look at some of the most crucial sections under the Privacy section in the Settings app.

Scan the QR code displayed alongside to download the Differential Privacy Overview PDF, which details the various techniques used by Apple to anonymize the data and the particular steps taken to ensure that the privacy of the user (and their data) remains protected.

[QR Code: https://www.apple.com/privacy/docs/Differential*Privacy*Overview.pdf]

Fortunately, Apple does make it (relatively) easy to opt-out of this data-collection. I'll explain how to opt-out of Apple's data-collection in detail, in the #RohitRecommends section towards the end of this chapter.

Diagnostics & feedback

Windows 10 users on the Pro, Enterprise, or Server versions have an option to switch off the collection of diagnostic data completely. Unfortunately, for users running the Windows Home version, this collection of data cannot be completely stopped but can only be restricted to a certain degree.

Sensors

Like all modern smartphones, all Apple iPhones come equipped with several sensors and radios that perform various important functions on your device. Along with the standard WiFi, GSM, and Bluetooth sensors, most modern iPhones also come equipped with Near-Field Communication, or NFC, chips to make payments using your iPhone possible. The latest iPhone (iPhone 11) also incorporates an Ultra-Wideband chip for spatial awareness.

Along with these standard radios , most modern iPhones (6 and upwards) also have several sensors that provide specific enhancements to your iPhone usage. For instance, proximity sensor, ambient light sensor, gyroscope, compass, barometer, Touch ID, and more.

Whenever active, these sensors and radios may share data in real-time with apps that might request them for their data, provided you grant them the necessary permissions for doing so.

While this seems to be a fairly trivial and seamless operation, I'd like to remind you once again that I've already described and demonstrated how these sensors can inadvertently leak data.

Therefore, as with Android, I would strongly urge you to keep your sensors switched off/deactivated until you legitimately need to use them, and then switch them off/deactivate them again when you are done. The details on how to achieve this are provided under the # RohitRecommends section at the end of this chapter.

Keystroke logging

First, go to the Speech, inking, & typing section under Privacy in the Settings app and click on the toggle switch next to Turn off speech services and typing suggestions . You'll still be able to use Windows Speech Recognition to some extent, but it won't be able to learn from you.

Permissions

Permissions refer to the requests made by an app to access the user's personal data on the device. These usually appear as floating dialog boxes whenever the app finds it necessary to request that permission.

Just like Android, Apple also allows granular permission control over the apps you install on your iPhone. When apps are installed on an iPhone, they are not granted any permission by default. All apps *must* acquire explicit permission from the user before accessing any private information on the device. These permissions are requested only as and when necessary. However, the permission granted is perpetual; although, you can modify or revoke these permissions anytime.

Unlike Android, Apple provides an additional level of granularity for the Location permission, where you can choose the Frequency with which GPS and location data is shared with the apps that request it. Apple provides three frequency-levels of access to GPS/location data: Always , While Using , and Never , which I am assuming are self-explanatory.

I would strongly recommend that you allow apps to access your GPS/location data only While Using . This will ensure that apps do not accidentally leak this information to any third-parties without your knowledge.

Cortana

Not many Indians are power users of the Windows operating system, that is, we do not rely on digital assistants to organize our day-to-day tasks and schedules. Therefore, I strongly recommend that you turn Cortana off entirely. Not being able to use Cortana won't make a noticeable difference in your Windows experience but turning Cortana off is likely to mitigate some privacy concerns, for sure certainly.

Info

This does not stop Windows 10 from reporting your search back to Microsoft, as ArsTechnica recently found out. The QR code given alongside this paragraph points to the ArsTechnica article, “Even when told not to, Windows 10 just can't stop talking to Microsoft.” Note that the article is from 2015, so some portions of the article may no longer be relevant.

The Settings App

One of the things that is different about Apple is the fact that all the important privacy settings and access permissions pertaining to every app installed on your iPhone are available under the corresponding sectionin the Settings app.

If you click on the section corresponding to an installed app, you can (usually)definitely find the following subsections:

Permissions: The various permissions that were requested by (and granted to) the app. You can drill down further and either selectively revise or entirely revoke these permissions.

Siri & Search: The toggle switches under this subsection allow various kinds of information from the app to appear in results provided by Siri and related search functions.

Optionally, the following sub-sections may also be present for some apps:

Background Refresh: This is a toggle switch that determines whether the app is allowed to perform its operations in the background, even when it is suspended.

App-specific settings: Each app may have its own set of settings for the user to modify.

Note that each app uses a different approach to populating their respective section under the Settings app. In some cases, this subsection may be completely empty for some apps (except for the Permissions subsection and the Siri & Search subsection), but there may be an entirely separate Settings page within the app itself.

[QR Code: https://arstechnica.com/information-technology/2015/08/even-when-told-not-to-windows-10-just-cant-stop-talking-to-microsoft/]

Analytics and Advertising

Compared to Google, Apple seems to take its stance on user privacy rather seriously. On its website, through various articles and support documents, Apple provides a rather transparent (and quite detailed) explanation about why and how it collects your data and what it does with that data.

I must admit, Apple seems to have gone out of its way to explicitly detail the various kinds (and amounts) of data it collects, on its website.

However, don't let this distract you from the fact that, if left alone and if left without intervention, Apple is likely to collect a bunch of data about (and from) your iPhone. I mean, for all the claims that Apple makes about being in the business of selling hardware and not your personal data, the fact is that it also sells ads through the Apple's Ad Platform. According to the support page detailing the Apple Advertising and Privacy policy:

Ads that are delivered by Apple's advertising platform may appear on the App Store, Apple News, and Stocks.

Scan the QR code displayed alongside this paragraph to check out the Apple Advertising and Privacy support page. If you have the time and curiosity, I recommend that you read it – won't take you more than 10 mins, I think.

Wi-Fi Sense

I recommend that you toggle Wi-Fi Sense OFF on your Windows 10 device. I also recommend that you do not share your Wi-Fi password with anyone -- not even your loved ones, not unless they are reading (or have already read) this book!

[QR Code: https://support.apple.com/en-us/HT205223]

Note

TL; DR for Apple's Advertising and privacy support document/page

If you are curious about what it says but are also lazy enough that you can't be bothered to scan the QR code, consider the following a quick, short primer on what the Apple Advertising and Privacy support page is all about.

Apple collects information pertaining to your device and usage, viz. keyboard language, device type, OS version, mobile carrier, connection type, device location, the searches you perform on the App Store, and the types of articles you read.

Apple creates segments, that is, groups of people who share similar characteristics, based on some of this collected information. Targeted ads are shown only if a segment has more than 5000 people.

The segments are further augmented using other usage and account data, such as your name, age, gender, address, downloaded content and apps, previously viewed ads, and many more.

Advertisers may further augment any data provided by Apple by matching it with data (for example, email, phone number, and many more.) they may have independently collected from the end user. While Apple tries to obfuscate as much as it can, Advertisers still have access to the Advertising Identifier, which they may use to categorize users into certain segments.

To explain it using a simple example, if less than 5000 people from your city search for music-streaming apps on the App Store using their iPhones, Apple will not show targeted ads from advertisers looking to target people interested in musicstreaming.

One thing that Apple makes abundantly clear is that they collect only usage data and not on-device data. Furthermore, they add random noise to this usage data so as to ensure that any personally identifiable information (PII) is overwritten and not directly accessible to the advertisers. Then, the data of several users is collected and separated into buckets of 5000 or more users. If a particular advertising category has less than 5000 users, the data is not made available to advertisers, thus reducing the possibility of fine-grained targeting of end users like you and me.

However, there is no end-to-end encryption involved, that is, the usage data that is transported to Apple's servers is not encrypted on the device, only during transit. Therefore, the possibility exists that a sufficiently motivated malicious actor could theoretically be able to access this data on your device.

Fortunately, Apple makes it rather easy to control what data is shared with Advertisers, in the Privacy section of your Settings app. You might not be able to stop it completely from collecting data, but you can definitely reduce the amount of data that gets collected. I'll discuss it in greater detail in the #RohitRecommends section of this chapter, of course.

Other 'Privacy' Settings

I recommend that you drill down into each one of these device options (or service options) in the sidebar, and toggle the various switches to the OFF position, depending on your comfort with the amount of data available and shared by each of them.

Specifically, if you own a laptop or have a webcam attached to your Windows 10 machine, ensure that you evaluate the privacy settings for the following sections in the sidebar:

Location

Camera

Microphone

Voice Activation

You might also want to look at all of the remaining settings and make of note of which programs have been provided access to which data on your device. If an app seems even slightly suspicious, toggle the corresponding switch to the OFF position. Better safe than sorry!

Info

OOSU 10

There is a third-party portable freeware called OOSU 10 (short for O&O Shut Up) which provides you with a single interface for toggling the various data-sharing options in Windows 10. It doesn't need to be installed and can be run from anywhere on your PC -- even a flash drive. You can download it here: O&O Shut Up10.

RohitRecommends

Those of you who read the first chapter carefully must have realized immediately that (anonymized or not) Apple's Differential Privacy policy still violates the third principle of data-sharing, viz. If the data is encrypted, but not in your control, then it might be secure but it is not private.

Therefore, my recommendation would be to reject Apple's telemetry as much as possible by toggling the appropriate switches under the Privacy section in the Settings app. Be aware, however, that this might seriously change your device usage experience, since Apple does rely on this data to give you a somewhat personalized experience on your device.

For example, the keyboard and typing analytics that Apple collects from your device contains details about hardware and OS specs, performance stats, and selected usage data—all anonymized and scrambled before uploading to Apple's servers. Apple then utilizes this data to improve the intelligence and usability of features such as QuickType suggestions, Emoji suggestions, Lookup Hints, and many more.

Here's what you can do to keep your personal data private and out of Apple's reach.

[QR Code: https://www.oo-software.com/en/shutup10]

However, the chances are that you won't need to do much here. One, most of the software that we use on Windows doesn't really make much use of these permissions. Two, the small number of apps that do end up using these permissions are usually ones downloaded from the official Microsoft store and therefore, mostly legit.

Personally, I have completely switched off app-access to all of the features listed in the sidebar (and not just the four named above) on all my Windows devices. None of the software installed on my machine uses this permissions framework, and the apps that do use this framework aren't of much use to me.

That being said, it doesn't hurt (and most certainly helps) to keep checking these permissions from time-to-time, to see if there are any unwanted apps that might be abusing any permissions, either accidentally or maliciously.

iOS and iCloud

If you haven't checked to see what data from your iPhone is getting backed up to iCloud, now would be a good time to take stock.

Open the Settings app and scroll down to the section titled iCloud . If you don't find a section titled iCloud , look for the section with your name. Click to open this section.

Here, you'll find toggle switches corresponding to various services such as Calendar, Reminders, Safari, Notes, and many more. Services with switches that are toggled ON are being backed up to iCloud, and services with switches that are toggled OFF are not being backed up to iCloud.

BASIC: (1 point)

Award yourself TOTAL of ONE point if you only read through all the recommendations made in this section

Figure 4.1: Accessing the iCloud options under the Settings app on your iPhone.

You can choose to either selectively sync the various apps and services listed here or you can stop your iPhone from syncing with iCloud altogether. Before you do either of them, you need to understand what either option actually does.

Take a look at the list of apps and services that are syncing data with iCloud and ask yourself the following questions:

Do any of these apps contain (or are likely to contain) any personal information now or in the future?

If someone else were to gain access to the app's data, what would they see? Am I worried about them seeing it?

If an app (or multiple apps) crashed, and all information contained within got deleted right now, would it cause you massive and irreparable loss?

Did you answer Yes to two or more of these questions?

INTERMEDIATE: (2 points)

Award yourself TOTAL of TWO points if you followed all the recommendations made in this section.

BASIC (1 point)

If you answered Yes to at least two questions, then maybe turning off iCloud syncing selectively on a per-app basis would serve you better than signing out of iCloud entirely.

Go through the list of questions and ask the question for each app. Then, depending on the answers, toggle the sync settings ON or OFF selectively for each app.

macOS

ADVANCED (3 points)

If you answered No to all three questions, then I strongly recommend you sign out of iCloud altogether. You can do this by scrolling down to the bottom and clicking Sign Out . This will stop your phone from syncing to iCloud entirely and none of your data will be automatically backed up.

BASIC (1 point)

Apple provides a bunch of configuration options to ensure the privacy of (most of) your data under the System Preferences application in macOS. The System Preferences can be accessed from the gears icon in the dock, or by going via the Apple menu | Preferences .

Click the icon labelled Security & Privacy and scroll through each section to understand how Apple collects and shares data from the various parts of your device. Pay special attention to the tab labelled Privacy and make a note of which apps have been given access to which of your personal information.

Next, you have a decision to make.

Sensors

Just like Android, device sensors on your Apple iPhone can be toggled ON or OFF. In case of Wi-Fi, Bluetooth, and mobile radio, the toggle switches for the sensors can be accessed by swiping up on the home screen or from their respective sections in the Settings app. However, the option to turn off Location Services can be found under the Privacy section of the Settings app.

Toggling these sensors off restricts apps from accessing the sensor data. This might result in some apps working incorrectly or not at all. For instance, toggling the Bluetooth sensor off prevents your Phone from connecting to other Bluetooth devices such as your car stereo or wireless speaker. Apps and services that rely on Bluetooth, such as AirPlay or ShareIt, might also not work as effectively or properly.

Similarly, turning off the location sensor prevents mapping apps and ride-sharing apps (for example, Uber, Ola, and Lyft) from working effectively. The Find my Phone feature also requires location services to be turned on for it to work effectively.

That said, toggling these sensors off helps in two important ways:

It greatly helps your device conserve battery.

It reduces potential attack surfaces for any potential adversaries.

It is definitely a trade-off, and you need to decide whether you want to toggle the sensors OFF or if you want them to remain toggled ON. If you can't come to a decision, here's my recommendation: open your Settings app and look at each sensor that is currently toggled ON, and ask yourself the question:

Is this sensor currently being actively used by an app?

Is the app being used (either actively or passively) by me?

INTERMEDIATE (2 points)

Once you have checked out all the sections under Security & Privacy in the System Preferences of macOS, toggle relevant switches as and where necessary, depending on the extent of Privacy you would like to maintain.

There may be some instance where you might need to leave a switch toggled on. For instance, sharing the contacts permission with the Spotlight feature may be necessary if you regularly rely on Spotlight to search through your contacts. However, at the same time, you might want to restrict Facebook from accessing the contacts on your macOS.

Check/uncheck the relevant checkbox to grant or deny permissions to the relevant services/features.

BASIC (1 point)

If you answered Yes to both questions, then leave it be – just remember to toggle it OFF once you are done using the app that is using the sensor.

For example, I'd recommend that you toggle the location services off when you are not using the Maps app/service. Toggle Bluetooth off if you don't have any Bluetooth devices connected to your iPhone.

EXPERT (5 points)

Scan the QR code given alongside this paragraph to be taken to an extremely detailed guide about macOS privacy and security is available on this GitHub page compiled by a GitHub user named DrDuh .

ADVANCED (3 points)

If you answered No to either or both questions, then I'd sincerely recommend that to toggle the sensors OFF .

For example, if you regularly carry your iPhone on your person, or if you are stationary (that is, at home or in the office), then keeping the Location Services toggled off will help you conserve your battery life. Similarly, I recommend that you toggle the Wi-Fi off when it is not being used, that is, when you step out of home or your office, for example.

[QR Code: https://github.com/drduh/macOS-Security-and-Privacy-Guide]

Be warned though, the guide is aimed at power users of mac OS, and it expects you execute console commands as a superuser. While I (and many other privacy experts and enthusiasts) find recommendations given in this guide to be quite useful, my lawyers insist I issue this explicit warning to you, dear reader:

“If you wish to follow the recommendations made in DrDuh's guide, please make sure you do so under expert supervision and know that you'll be doing so at your own risk!”

Permissions

To modify or revoke permissions for an app, you can open the Settings app and either:

Scroll down and click on the section corresponding to the app.

Open the section titled Privacy and click on each permission sub-heading.

Like Android, Apple too provides easy access to toggle these permissions ON or OFF. The following image shows a screenshot displaying the various headings seen under the Privacy section in iOS 12.3.1.

Linux

Linux is generally considered a highly privacy-aware (if not privacy-focused) operating system. Most Linux distributions usually transmit little to no telemetry data from your devices.

However, a recent case has forced long-time Linux enthusiasts to question this belief.

Around three years ago, in late 2014, users of Ubuntu were surprised to discover that searches performed using the Unity Dash (a search bar built into the Ubuntu Desktop Manager) would return results featuring products you could buy from Amazon. At the time, Canonical categorically stated that all search queries were routed through Canonical's servers to Amazon and other search partners, and not directly as was being assumed.

In light of the controversy that followed, Ubuntu first resisted and finally relented by redesigning the search feature in Unity dash to make it separate and configurable, that is, searches in Unity dash would remain on the local system, and any external search capabilities would have to be 'installed' as plugins to be made available to the users.

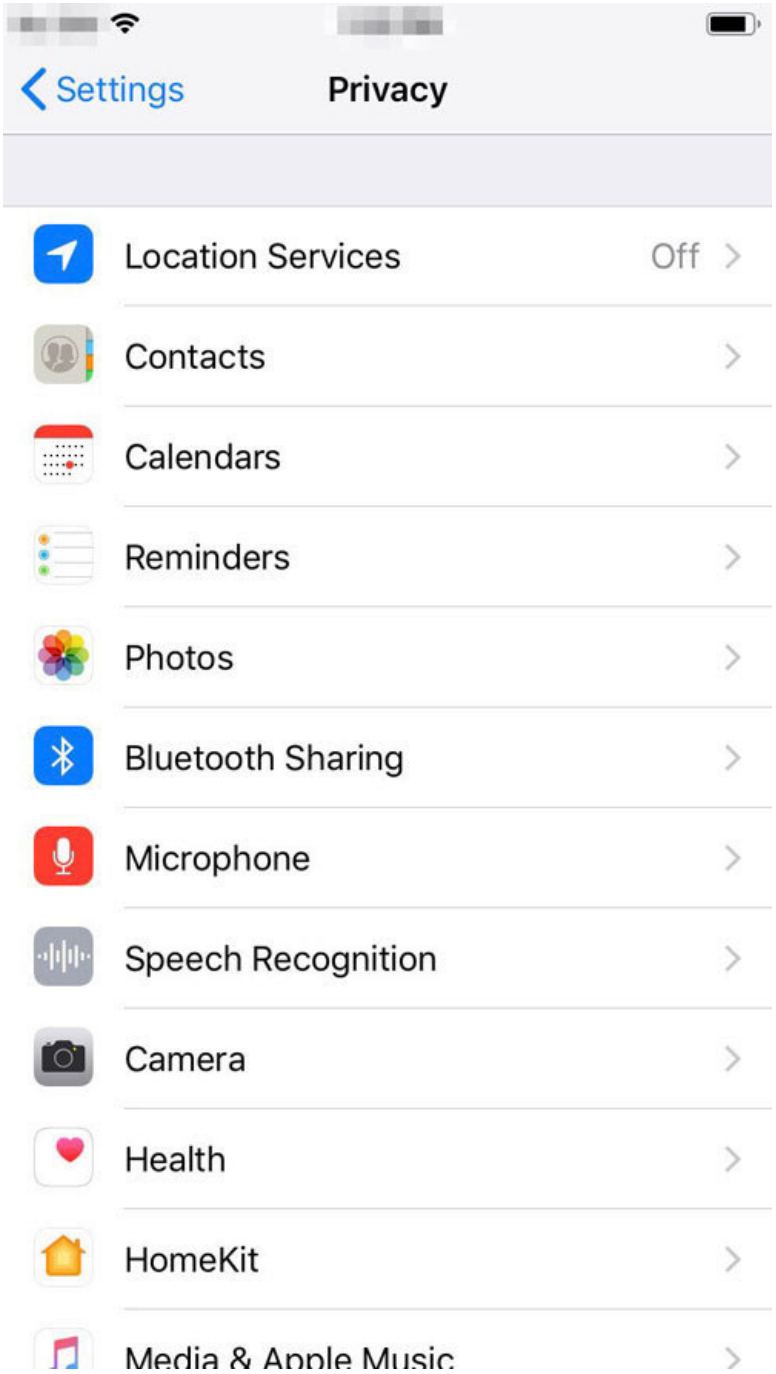


Figure 4.2: The 'Privacy' section in the “Settings” app seen on an iPhone 6s running iOS 12.

Like we did with sensors, we first need to understand which of these permissions are inconsistent with the app's usage before we can opt to modify or revoke them entirely. So, as you drill down into each permission sub-heading, ask yourself the following questions:

Is this permission absolutely necessary for this app to function?

Am I okay with this (permission-specific) data being shared with this app?

For the Location permission, am I okay with the frequency with which the app can access location data?

Once you have answered these questions, proceed to the next step to figure out which recommendations you might able to follow.

BASIC (1 point)

Among the popular Linux distributions, Ubuntu is known to collect and transmit some telemetry data back to its servers through the following packages and/or (associated) services:

ubuntu-report: Collects and reports information back to Ubuntu [8] at the end of OS installation.

popcorn: A package that tracks the relative popularity of apps and packages installed by other Ubuntu users.

apport: A package that automatically sends anonymous crash reports back to Ubuntu.

whoopsie: A package that sends the crash reports generated by apport to Ubuntu, but only with your explicit permission.

BASIC (1 point)

If you answered Yes to all the questions, then there isn't much to do here. You can skip the rest of the recommendations and safely proceed to the next section.

ADVANCED (3 points)

If you are an Ubuntu user, search the internet on how to remove the following Ubuntu packages. There are several articles explaining what each of the packages does and how you can safely prevent them from conducting any telemetry.

However, if you are absolutely sure you want to remove them from your Ubuntu system, and if you are comfortable running commands in a terminal, you can simply run the following apt command to remove all packages from your Ubuntu installation:

$ sudo apt purge ubuntu-report popularity-contest apport whoopsie

Additionally, you can block access to metrics.ubuntu.com and popcon.ubuntu.com using the inbuilt firewall or any other firewall of your choice.

ADVANCED (3 points)

If you answered No to any of the questions above, you might need to (re-)evaluate your use of the app and the permissions being granted to the app.

If the app can still function after being denied some permission, then you might want to try toggling it off and see how it impacts your usage of the app. If the data being shared with the app contains some very personal information, then you might want consider not using the app or using a different one.

The frequency only matters for the Location permission and, as I mentioned earlier, toggling it to While Using should be more than enough for most apps.

As an example, let's look at one of the most popular apps on the App Store—Instagram. By the time you set it up and use it regularly, Instagram will have requested for and (most likely, be granted access to) the Location, Photos, and Camera permissions.

The following image shows a screenshot of what the Instagram settings screen might look like on your iPhone after navigating these permission requests:

Conclusion

Just like with smartphones, computers are also usually identified by the operating systems that run them. Broadly speaking, you are likely to use a Windows computer, a Mac, or a computer running a Linux-based operating system.

The focus on operating systems' capabilities to protect (or infringe) upon your privacy has come into sharp focus recently with certain revelations about Windows 10. Several security and privacy experts found that Windows 10 was an extremely intrusive OS, with numerous privacy-infringing settings turned on by default.

However, Windows isn't the only operating system that collects usage data -- both macOS and Linux are also culpable of it to some extent, although not as much as Windows. In any case, I hope this chapter has given you an idea of the length and breadth of data that you are currently sharing with the developers of your operating system.

Now, I understand that it is quite difficult to switch operating systems at the drop of a hat. However, I believe that, as a privacy and security expert, I have a moral obligation to inform you of the risks of continuing to use the Windows operating system without-- especially, when it has historically been a large surface area for attacks by adversaries.

Oh, and one other thing: all the telemetry options described in this chapter assume a clean installation of the OS. As you install/add new applications and games to your desktop machine, they may conduct their own telemetry, which may be overt or covert. Spend a little time poking around in the various settings of the application and see if you can spot the telemetry settings.

In the upcoming chapter(s), we'll look at some commonly used applications, the kinds of data they are known to collect, and the different ways to

deal with it.

---

[1] This is likely to change soon, since Microsoft has stopped providing support for Windows 7 after January 2020, which was the declared end-of-life date for Windows 7. Organizations may still opt for the extended license, which will provide them with Windows 7 support for another three years, until 2023.

[2] A Unix-like operating system descended from the Berkeley Software Distribution

[3] SPOILER ALERT: This statement is untrue. Macs most definitely do get viruses, albeit fewer than Windows.

[4] MacOS systems have a provision for a 'super user' named "root" that is granted all privileges on the system but it is disabled by default. Keep it disabled. Do NOT enable it for any reason whatsoever.

[5] While I do not deny that telemetry does have its uses, I oppose any telemetry that does not provide a mechanism to opt-out. Non-consensual telemetry, in my opinion, is a violation of my right to privacy.

[6] At the time of writing this chapter, this was v1903, popularly referred to as the May 2019 update.

[7] As of the date this chapter was written, the latest available version of Windows 10 is 1903. Windows 10 version 1909 (scheduled for release in November 2019) may be the latest version by the time you are reading this.

[8] Well, the reports are sent to Canonical but that's one and the same, you know?

Figure 4.3: To access this screen on your iPhone, go to Settings | Instagram

You'll notice that some permission such as Camera and Photos are absolutely necessary for the app to work. However, the Location permission is only required if you want to geo-tag your posts.

Here's the thing, even if you toggle the Location permission to Never , you'll still be able to geo-tag your posts by searching manually for the location before posting your photo to Instagram! Of course, this means you are now voluntarily sharing your location data with Instagram. However, this defeats the purpose of the whole exercise, viz. maintaining the privacy of you and your data, so I'd recommend against doing it.

Chapter 8

Desktops-Software Applications

Settings | Privacy

Simply speaking, what Android calls dangerous permissions, Apple calls Privacy settings. These Privacy settings can be accessed by opening your Settings app and scrolling down to the section named Privacy . Tap on it to open it.

Broadly speaking, the headings under this section can be classified under the following five categories:

Location sensors: Options to toggle the Location Sensor ON or OFF.

Personal data (text): Contacts, Calendars, Reminders, and Bluetooth Sharing.

Personal data (non -text): Photo, Camera, and Microphone.

Smart devices : Home, Health, and Motion and Fitness.

Analytics and advertising: (self-explanatory).

The fundamental concepts behind these permissions are the same as that on Android. The names may be different but the ideas are very much the same. In fact, you might want to read the section in Chapter 15 , titled, “The 10 Android permissions listed under 'dangerous' protection-level” for a brief discussion of what these permissions mean and examples of typical/atypical apps that might request these permissions.

BASIC (1 point)

If you drill down into each of the sections one-by-one, you'll find a list of apps that have requested the corresponding permission. The toggle switch next to each app indicates whether or not the app has been granted that particular permission. If you change your mind after you grant permission, you can restrict (or entirely revoke) these permissions by toggling the switch next to a specific app, much like you would do in Android.

For instance, you may want to give location permissions to apps only While Using and not Always . Or you might want to revoke Facebook's access to your address book by toggling the switch next to Facebook under Settings | Privacy | Contacts to the OFF position.

Introduction

While most operating systems these days come equipped with several programs that can read and display all kinds of files, it is virtually impossible to use a desktop without installing any third-party programs.

Take Windows, for instance. Windows comes pre-installed with an internet browser, a music player, an email client, and a bunch of other software that provides the capabilities to read the most common file-types such as ZIPs, TXTs, DOC/DOCXs, PPT/PPTX, and many more. However, most of us rarely use these inbuilt options. It is quite possible that you use Mozilla Firefox (or Google Chrome) as your browser, VLC as your music player, and Mozilla Thunderbird as your email client.

In fact, forget the applications , just answer me this: can you use a Windows machine *without* installing any games on it? Yeah, that's what I thought.

When you install a third-party (read: non-Microsoft) software application on your machine, you increase the probability of exposing some vulnerability on your system. Additionally, if these third-party software applications have the capability to connect to and interact with remote servers, the risk to your privacy is also higher.

In this chapter, we'll look at the concept of third-party software applications that we tend to install on our system and how some of them can have adverse effects on our system and our privacy. We'll also look at the concept of security software which can help mitigate some of these threats.

Analytics and Advertising

For what it's worth, Apple does provide a very easy method to turn off all Telemetry and Analytics for users who wish to opt-out of Apple's datacollection.

Open your Settings app, and scroll downto the section titled Privacy . Then, scroll all the way down to the bottom where you will see two subsections titled Analytics and Advertising .

The following image shows a screenshot of what the Analytics and Advertising Settings screen might look like on your iPhone:

Software applications

Before I describe how various software applications can affect your privacy, I'd like to lay down a few definitions:

Authorized software refers to a software application present on your system that has your explicit permission and the proper license required to run it on your system.

Unauthorized software refers to a software application present on your system that does not have your explicit permission OR [1] the proper license required to run on your system.

Essentially, software applications (or programs, as they are commonly referred to) take your input, process it, and provide the output you desire. The word processor, on which this book was written, took the input from my keyboard and mouse and made the last word of this sentence bold . When you visit a website, the browser takes input from your keyboard and mouse and shows you the result in the window, usually in the form of a webpage.

Could you tell me the different points in the process where your personal data could possibly leak in the above examples?

If you said anything close to all points where information is being transported, you would be absolutely right. There are two transport points in the above examples:

Between the input and the processing stage.

Between the processing and output stage.

Of course, if each of the stages has sub-stages, then the transition between those stages is also a potential source of dataleakage. For example, extending the website example, when signing in to a website in a browser window, your password is sent from the browser to the remote server. If this password is not encrypted and someone just happens to be eavesdropping on your internet traffic, your password was just leaked to an unauthorized third-party.

I'm not saying that all programs installed on your system will always leak data or that any and every application you install on your system makes your system immediately vulnerable. However, each new program you add to the system brings with it its own three stages of input, processing, and output, that is, its own points of data leakage.

In fact, the more popular a program, the more likely it is that it will get exploited by malicious actors. Some of the first viruses were transmitted through improperly secured macros in Microsoft Word. There have been several vulnerabilities in Adobe products (Flash, Acrobat, and Reader) over the years that allowed malicious code to be executed remotely on users' systems.

Note

Unauthorized Software andPiracy

Not all software applications directly ask for your password. However, they do have virtually unrestricted access to your system and to most of the files on your system. By allowing them to run on your system, you are essentially declaring that you trust the program not to conduct any malicious activities on your system. By extension, you are saying that you explicitly trust the developer of the program not to include any malicious code that could affect your system, and/or the privacy of your data.

Here's my question to you: can you honestly say that about ALL the programs that you have installed on your system? Even pirated software?

Pirated software is software that has been modified by someone who is not the original developer to force the software to operate outside its licensing conditions. If you are using a pirated software that requires a payment to function otherwise, you are using it in violation of the agreed terms and conditions.

There is another problem with pirated software: whoever modifies the software to bypass any restrictions also has the capability of inserting additional malicious code. Furthermore, the sites that host such pirated content are known to be filled with several advertisements, a lot of which are links to malware. Even the content can be (and often is) severely riddled with malware.

I'm not judging anyone for using pirated stuff -- that's a different discussion, for a different book, for a different day. For all I know, you might even have downloaded THIS book as a pirated PDF or EPUB!

All I'm saying is while piracy may help you save some money, the eventual cost of piracy can be extremely high, so, just be careful!

Bloatware

Chances are, you might have come across an antivirus, or a game, or a backup utility, or a manufacturer-branded Control Centre installed on a brand-new PC. Some manufacturers will even install full versions of third-party utilities on a brand-new PC. While these programs and utilities are not really essential for the operating system, they, sometimes, do provide additional functionality to users.

These days, operating systems usually ship with a bunch of additional programs and utilities. Especially, with recent versions of Windows (starting with Windows 8 and up), Microsoft began bundling multiple apps such as Bing News, Bing Maps, and many more, along with its standard installation of Windows. On top of that, manufacturers often add their own tools and utilities, with assorted third-party tools and utilities further adding to the clutter in your OS.

Thus, even before you boot your desktop PC or laptop for the first time, you are already saddled with a ton of apps, utilities, tools, and programs that you are unlikely to ever use in your life. Not only do they add to the clutter and consume resources, but some of them may end up actively harming your system and sharing your data with thirdparties without your explicit consent.

For example, in Jun 2019, a flaw was discovered in Dell Support Assist, the troubleshooting software that comes pre-installed with most Dell PCs and laptops. This flaw was so severe that it could allow malicious users to gain complete control of a vulnerable device. Since most users don't pay much attention to (read: upgrade) such as pre-installed bloatware, it was very likely that a significant number of Dell PCs and laptops may still be affected.

For purposes of this guide, I define bloatware as all programs (third-party or otherwise) that are inessential to the core OS but are bundled with the default installation anyway.

Bloatware on desktops can be typically classified under one of three categories:

Manufacturer-branded utilities

Third-party apps and games

Integrated bloatware

Let's take a look at each one of them and delve into greater detail.

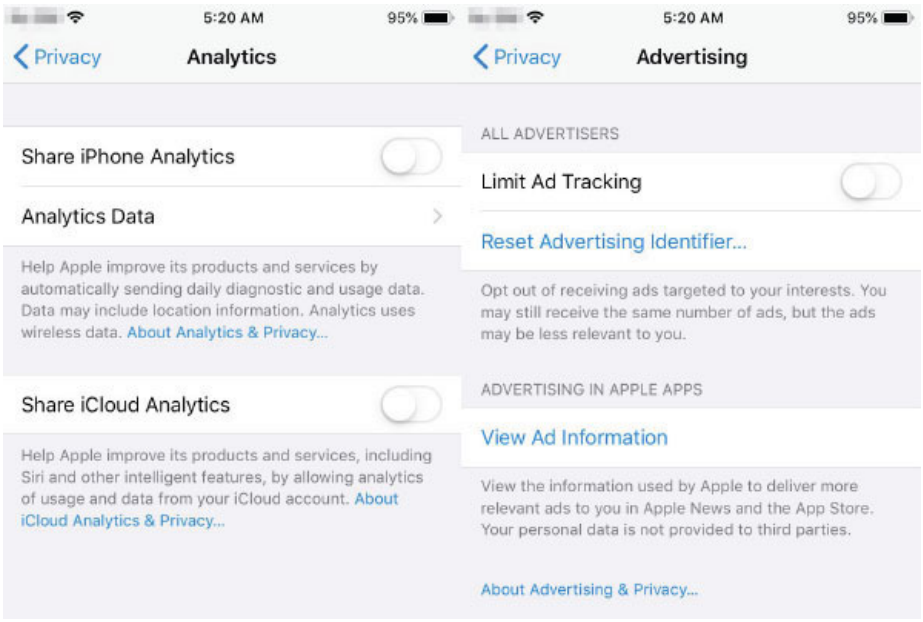


Figure 4.4: The Analytics and Advertising sections under Settings | Privacy.

The Analytics section allows Apple to collect your usage data on a daily basis, while Advertising refers to the data collected by Apple for targeted advertising, subject to the collection methods described earlier in this chapter. Here is a quick description of what you can expect to find under each of these sections:

Under the Analytics section, drilling down into Analytics Data shows you all the data that was sent to Apple. You can also read more about Apple's stance on data collection for analytics by clicking the link titled About Analytics & Privacy under the Analytics Data section.

Under the Advertising section, clicking on View Ad Information brings up a window with details on the information collected for targeted advertising from your device by Apple. You can also read more about Apple's stance on data collection for targeted advertising by clicking the link titled About Advertising & Privacy … at the bottom.

While Apple claims that none of the collected information identifies you personally, I say you can never be too careful.

Manufacturer-branded utilities

If you bought your Windows PC from a manufacturer like Dell, HP, or someone similar, chances are you'll find some manufacturer-branded software on your systems. For example, Dell laptops ship with a utility called Dell Support Assist, which allows you to connect with Dell Support when you run into issues with your PC.

Typically, most PCs and laptops ship with manufacturer-branded utility software in order to help maintain your PC. However, this utility only serves a purpose as long as you are registered with Dell Support and within warranty. Once your warranty expires, you are required to purchase an additional warranty to get official support from Dell. Moreover, these utilities are configured to send back various kinds (and amounts) of data about your system to the manufacturer's servers. This is done, ostensibly, to maintain a record about your system and registration with the manufacturer.

In other words, a manufacturer-branded utility serves its purpose for only a limited amount of time and can result in additional expenses and additional data-leakage for the rest of the time.

Here's the thing, though. Almost all the major versions of Windows (Windows 10, 8.1, 8, 7, and even XP) come with similar, in-built utilities that help you maintain your PC. A quick search on the internet will provide you with a solution for your issue that makes use of these in-built utilities instead of manufacturer-branded ones, in almost all scenarios. Depending on your knowledge and technical expertise, it might be either easy or messy to deal with but (in a majority of cases) it won't require you using the manufacturer-branded utility.

Manufacturer-branded utilities may insist that they serve a purpose for the average users of the world. If you were an average user, we'd probably be okay with you letting these utilities exist on your system. However, as a reader of this book, you have clearly indicated that you'd like to improve the security and privacy of your data. I therefore strongly recommend uninstalling these utilities from your Windows PC and laptops.

BASIC (1 point)

Open the Analytics section and toggle all the switches to the OFF position, as displayed in the figure. Note that this screen is likely to look different if you are on a different OS version and if you have an Apple iWatch paired.

Next, open the Advertising section and toggle the Limit Ad Tracking switch to the OFF position. Click the Reset Advertising Identifier … link below that and then Reset Identifier in the confirmation message that appears.

This set of actions ensures that all the previously tracked ads will be dissociated from your account and a new identifier will be assigned to your account, which essentially wipes your ad-tracking slate clean from an advertising perspective.

I strongly recommend that you do this every three to six months to prevent advertisers from building a comprehensive customer profile for you.

Info

Limiting adtracking and resetting the advertising identifier simply means that Apple won't be able to use your usage data to tailor the ads it shows you. Apple will *still* show you ads, only that they are likely to be less relevant.

Third-party apps and utilities

Some manufacturers and vendors will include additional applications and/or utilities as a part of the package for the desktop or laptop when you purchase it. For instance, they may include a trial version of a popular antivirus, or a cloud backup service such as Dropbox, or photo-editing software.

With recent versions of Windows, Microsoft has been including various popular apps such as Netflix, Facebook, LinkedIn, Dropbox, and sometimes Suggested Apps such as Candy Crush, and enhanced versions of Solitaire and Minesweeper.

Note

The decision to display Suggested Apps that has been implemented in Windows 10 is devious and distasteful, in my personal opinion. Some of these Suggested Apps appear as a tile in your Start menu, but they aren't actually installed by default. When you click on the tile, you are taken to the Microsoft Store page where you are prompted to install the app on your machine.

Technically, the app isn't installed by default; the installation always happens *with* your consent. However, the fact that it appears on a tile in your Start menu leads you to believe that the app is already on your machine, thus making the whole thing a shade greyer than a 'false' advertisement.

Like I mentioned earlier, you might actually find some (or even all) of these utilities useful. Therefore, it is important that you make a note of all such applications and utilities on your system and figure out for yourself, which of these utilities you absolutely need and which ones you could do without.

In some cases, some of these utilities may not be as benign as they look. Some vendors have been known to ship systems riddled with various

kinds of adware, spyware, and other malware -- either on purpose or by accident. I don't have to tell you that adware is not only irritating but it also often ends up slowing down your system. In some severe cases, it can even end up sharing some (or all) of your confidential data with third-parties.

Thankfully, most of these can be easily uninstalled -- I'll tell you exactly how to do it in the #RohitRecommends section further ahead.

INTERMEDIATE (2 points)

If you haven't done it already, I'd strongly recommend that you turn on 2FA (Two Factor Authentication) for your Apple ID. To do this:

Open the Settings app and go to [Your Name]| Password & Security .

Tap on Turn on Two-Factor Authentication and then tap Continue .

Enter and verify a trusted number.

The last step, where you need to enter and verify a trusted number, is a one-time process. Apple sends a verification code that you will need to enter to verify your phone number and turn on 2FA for your Apple iPhone.

There are no further recommendations because this is both the bare minimum that I recommend for everyone and the maximum that Apple provides in terms of pro-active user-input.

Secondly, unlike Google, Apple does not provide a portal to manage your historical data, that is, data that you have shared with Apple until now. Therefore, all data that you have previously shared with Apple remains shared for Apple to use as they deem fit.

Thus, the only thing that you CAN do is to take the proactive steps mentioned above and hope that both Apple's privacy policy and its servers are secure enough to prevent your data from getting breached.

Conclusion

Apple devices pose a very interesting conundrum.

On the one hand, they certainly seem to have the more user-friendly options for users to take control of their privacy. However, Apple never fully cedes control to the user.

For instance, all Apple devices come with granular controls to prevent apps from snooping on your data. Apple imposes strict guidelines (read: restrictions) on developers in terms of what data they can and cannot access from the user's iPhone. Apple actively prevents users from installing jailbreaking software.

At the same time, Apple doesn't really allow you to access/modify/delete any historical data. All of your attempts to control your privacy exist only in the moment where you try to control it. Furthermore, a lot of the actions that Apple executes in the name of protecting your privacy , seem to have no associated feedback mechanisms, that is, there is no way to check whether the executed action truly had the intended effect.

In short, while Apple seems to have a robust mechanism for protecting their users' privacy on their device, most of it seems to heavily based on trust rather than transparency.

At the end of the day, all of it boils down to one simple question: Do you really trust Apple to respect your privacy and the privacy of your data? How much?

---

[1] The story goes that Steve Jobs was the one who constantly pushed the Apple engineers to make their products look stylish and sexy, while keeping their essence and operation simple and to the point.

[2] Technically, Apple ‘designs’ the handset and outsources it to the Chinese manufacturer Hon Hai (English name: Foxconn) who manufactures the actual handset at its factories elsewhere in the world.

[3] SPOILER: The answer is, a rather underwhelming, “Maybe.”

[4] As of writing this book, an open-source jailbreaking tool called ‘ipwndfu’ that could potentially allow jailbreaking millions of iPhones, was being actively researched & developed by an anonymous security researcher called axi0mX.

[5] You can even take a look at what data is being shared from your iPhone under Settings > Privacy > Analytics > Analytics Data, in the entries that begin with Differential Privacy.

Chapter 5

Smartphone Apps

Introduction

According to data made available by AppAnnie , in 2018, consumers downloaded 194 billion apps in total, spent $101 billion (up 75% from 2016) in apps stores, and averaged three hours a day on their mobile phones. That's more than the money people spend on music (live AND recorded), twice the amount of money people spend on sneakers, and three time the size of the oral care industry! It is estimated that app store consumer spend will surpass $120 billion in 2019—double the size of the global box office market!

According to data made available by AppBrain , as of February 2019, the total number of iOS apps available was around 2.2 million. Google Play store reportedly had over 2.7 million apps as of July 15th 2019. Of these, a little over 57% of apps use an ad network.

On average, smartphone users have about 80-90 apps installed on their phone and launch an average of between 5 and 9 apps a day, and more than 30 apps on a monthly basis. This trend, surprisingly, has remained consistent since 2015 and is now known as the 30:10 rule, that is, 30 apps a month, 10 apps a day.

Integrated Bloatware

In some cases, the manufacturer-branded utilities might be so tightly integrated with the operating system itself that the uninstall option might not be available at all. This is typically seen with some default Microsoft applications like the Edge browser, or the Groove Music app in Windows 10 installations, or with some manufacturer-branded software on Windows installations.

Unfortunately, not all manufacturer-branded software is designed to be perfectly secure. If a malicious actor were to compromise them, it could result in severe consequences for you as a user, as was evidenced with the Lenovo-Superfish fiasco between 2014 and 2016.

Info

The Lenovo-Superfish Debacle

In 2014, Lenovo announced that its notebooks would come installed with Superfish, a technology that would help users find product offers by analyzing and matching product images while you were surfing the internet.

In other words, Lenovo had installed a piece of software that could intercept your encrypted communication and directly inject ads, based on what you were browsing.

Not only was this a gross violation of privacy, but if this technology were to be compromised by malicious actors, it would serve as an easy way for them to intercept any and all encrypted communications.

What's worse is that Lenovo initially tried to downplay the severity of this behavior by claiming that they weren't monitoring user behavior or recording any profiling information. However, all that changed when researchers from Errata Security presented a proof-of-concept to intercept communications using Superfish software maliciously. In case you are curious, the Errata Security researchers cracked the encryption on the certificate that was at the centre of this mess. You can read the details of how they did it over at their blog by scanning the QR code given alongside this paragraph.

After getting significant backlash from the security community, Lenovo was forced to declare Superfish as vulnerability and provide its customers with removal instructions.

Bloatware

When you switched on your smartphone for the first time, you probably saw a bunch of apps that are not a part of the official operating system, i.e., apps that are not critical for the operating system to function. Some of these apps may even be really popular apps, for example, Xiaomi bundles the Facebook app with MIUI on most of its phones. Apple bundles the Stocks app on iPhones.

For the purposes of this book, I will be defining bloatware as an app that is not a part of the core operating system or actively installed by the user, regardless of its popularity. In some cases, users don't even have the option to remove the app– only disable them! Most users neglect them and they continue to remain on the phone, hogging valuable system resources.

[QR Code: https://blog.erratasec.com/2015/02/extracting-superfish-certificate.html]

Such integrated bloatware can be difficult to uninstall, but it is certainly not impossible. It definitely requires a certain degree of alertness and cares that I have detailed in the #RohitRecommendations section below.

Security software

Given how common internet usage is these days, all desktop devices need a proper security system installed on them to ensure that your personal data stays on the PC. This typically involves installing and setting up a firewall and antivirus software on your machine, more so if your machine is Windows-based.

Of late, due to the rapid increase in malware attacks, installing anti-malware software makes more sense than installing an antivirus. In fact, most antivirus programs also provide malware detection and removal capabilities by bundling all features under one single security suite of sorts.

Let's take a look at each one of these software applications and what they actually do.

Firewalls

A firewall is simply an application that looks at every port and monitors the packets of information that is sent or received by each one of these ports on your system.

How to Identify Bloatware on Android?

Typically, apps on a smartphone can be broadly divided into two categories – (pre-installed) system apps and downloaded apps.

Say, you have a hundred apps installed on your phone, including the apps that were already installed when you bought the phone. Let's try and isolate the different categories of apps that you are likely to use, shall we?

Hourly usage: Email, browser, messaging (for example, WhatsApp, Signal, Facebook messenger, Telegram, and more).

Daily usage: Games, social networking (for example, Facebook, Twitter, Instagram, Snapchat, and more).

Weekly/monthly usage: Payments, banking, and more.

Random usage: Productivity, tools (for example, calculator, the camera, the clock, contacts, and more); settings; maps; shopping; entertainment (for example, Netflix, Amazon Prime Video, Saavn, Gaana, Spotify, and more).

Hopefully, you were scrolling through your apps while reading the bullet points above. Did you notice any app on your phone that did NOT get accounted for in the previous paragraph? Those are the apps that you need to look at and ask the following questions:

Do I need this app at all?

If I don't need it, can I remove it?

If I can't remove it, what exactly is it doing on my phone?

If you answered, "Uh, I downloaded that app when I was bored and looking for something but I forgot to uninstall it," then now would be a good time to uninstall that app.

If you answered, "Android won't let me uninstall this app because it is a 'system' app," then it is likely to be pre-installed bloatware that you don't need.

In either case, chances are that the app is probably collecting information and sending it somewhere.

Malware

While bloatware refers to apps that come pre-installed on your phone, malware (short for malicious software) refers to those apps that are primarily designed with the intent of stealing or damaging your device and data.

Antivirus and anti-malware

An antivirus software (or AV software) is a program that can scan, detect and prevent the proliferation of viruses on your system. Viruses are programs that replicate themselves by modifying other programs and inserting their own code, much like their biological equivalents.

These days, however, due to the increased threat of different kinds of malware (such as adware, ransomware, botnets, and many more) most AV

software also provides anti-malware capabilities, so it makes sense to club both of them together. If anything, viruses are now considered a subset of malware, but the language used to refer to them is often used interchangeably by most AV developers.

RohitRecommends

Regardless of whether a program is authorized or unauthorized, malicious actors will often try and exploit known and unknown vulnerabilities in the most commonly used programs to try and gain access to a system. Most software developers will issue updates to their programs to patch these vulnerabilities, but it is your responsibility as a user to ensure that you keep your software updated.

So, is updating programs enough to keep malware at bay? How do you protect your data from being leaked? How do you ensure the security of your system and your data? Is not using pirated software enough to avoid being infected by malware?

The short answer is: There is no singular approach that just works .

There are several steps that you must take to ensure that your data remains secure on your system. I'll try and outline them as best as I can but, keep in mind because security is a continuous process, this list will never be 'final' in any way, shape or form.

What are the Different Kinds of Malware?

The most common types of malware that can affect your device are viruses, Trojans, spyware, ransomware, and many more.

Viruses are malicious programs that replicate by attaching to another program. However, most modern phones such as Android and iPhone cannot *technically* have viruses because each application on Android runs within its own 'sandbox', that is, it cannot exchange any data with other apps unless explicitly given permissions (or privileges) to do so.

Spyware and Trojans are the most common forms of malware that affect Android users. Malware of both these kinds usually install hidden services that are able to collect and send your personal data to thirdparties without your consent.

Ransomware is a kind of an application that locks the user out of the device, that is, holds them ransom. In some cases, it may take over your device and encrypt it further. The users will remain locked out until a payment is made to some anonymous cryptocurrency account, after which a decrypting mechanism/key may be provided to unlock the device.

Info

The Android PNG Malware Exploit

For a long time, it was believed that you could not get malware on your phone unless you actively made a choice to install it. However, all that changed early this year (February 2019) when Google disclosed in its security update that there was a flaw that could allow a malicious actor to install malware on a target phone by simply sending a PNG image.

That means your phone could be infected with malware just because you innocently tried to open a malicious image. The situation becomes even worse when you think of the many ways in which this can happen accidentally.

Although Google fixed the vulnerability in February itself, the fix has not been pushed to all Android devices. If you want to check whether your phone is up-to-date and protected against this vulnerability, you can do so by following these steps:

Open your Settings app.

Scroll down to the bottom and open the About Phone section.

Check the Android version, specifically the date mentioned under the subsection titled Security Patch .

If the date happens to be a date *after* February 2019, you can consider yourself protected from this vulnerability. If not, consider upgrading either your operating system or your phone, at the earliest.

Software applications

BASIC (1 point)

It only takes a single vulnerability in a program to expose your data and render it vulnerable to unauthorized access. That said here are some basic rules [2] that you must set for yourself to ensure the bare minimum privacy of your personal data.

I can't begin to tell you how many times I have been invited to conduct security workshops in offices and found login credentials written on post-its and/or pinned to a softboard in the cubicle. DON'T. DO. THIS.

Always work under the assumption that someone else can ALSO see the text that you are typing into your computer.

If something seems too good to be true , it probably is. That means you haven't won the Coca-Cola lottery and you aren't the one-millionth visitor to a website. No, you won't be able to buy an iPhone by bidding the lowest. The government isn't giving free money, and the Nigerian guy is definitely scamming you.

If a webpage looks suspicious , close it immediately. By suspicious I mean, if a webpage has more than one download button, or wants you to 'complete a survey', or 'hit the monkey', or do some similarly stupid thing to download a file, close it immediately. If a webpage tells you your browser doesn't have a plugin [3] , ignore it and close it immediately.

Update all your programs and update them regularly. You can protect yourself against known vulnerabilities that have been patched by the developers of the software.

Make sure you have adequate security software viz. firewall and antivirus/anti-malware installed and active on your system, and ensure that it is up-to-date with the latest patches and definitions. We'll be discussing these in detail a little later in this chapter.

Encrypt your personal files, especially the ones that have your personal and/or financial information in them. Also, lock your screen before you leave your chair. Log out or shut down your machine if you are leaving for an extended period of time.

Avoid using unauthorized (that is, pirated) software, if possible.

Vulnerabilities are basically 'holes' in the software that can be exploited by attackers to access data on the system without your consent. Patching all the holes properly and quickly is necessary to prevent attackers from exploiting them.

How Do I Know I'm Affected?

A malware infection on your device can be likened to your device being ill —you will immediately know that something is not right.

Your device may suddenly start acting sluggish, freeze occasionally, or throw up some junk on your screen. Or you may find the browser displaying random websites with suspicious-looking URLs in the address bar. Ads may pop up at random times and you may find yourself being subscribed to random paid services without your knowledge and/or intervention.

Info

Malware is NO Child's Play!

A white-paper by Rubica published in February claims that kids are a lucrative target for cybercriminals. One, their lack of knowledge combined with a casual attitude makes then vulnerable to clicking random ads, which might install malware-by-proxy. Two, their behaviors can be manipulated by cybercriminals to acquire wider and/or deeper access to their parents' data—since most parents often share their devices with their kids.

In fact, the Rubica whitepaper found that some of the most popular kids' games often displayed aggressive interaction behaviors, such as excessive ads, unsafe download prompts, invasive permissions that grant access to device logs, history, location, microphone, etc. This set of behaviors shares multiple similarities with the behaviors of cybercriminals trying to access personal data of targeted users. Popular games such as Fruit Ninja, Talking Tom, Angry Birds, and more, were evaluated and found to be unsafe enough to require parental supervision and intervention from time-to-time.

Scan the QR code given alongside, in this info box, to read the entire white paper on the Rubica website.

INTERMEDIATE (2 points)

Before installing a program, ask yourself the question. Is the developer of this program (individual or company) trustworthy?

While installing a program, pay close attention to the descriptions in the installer window, especially when the installer asks you to make a choice. Programs downloaded from unofficial sites will often include a checkbox to install a secondary product, for example, a free antivirus which is actually malware disguised as antivirus. If any of the descriptions sound confusing, exit the installation immediately and consult with someone who can guide you through the process.

Monitor your security software (that is, your firewall and your antivirus/anti-malware) regularly for any and all kind of suspicious activity. If you spot a program sending a lot of data, consult with an expert as soon as you can.

Most programs will display a notification when something needs updating. However, if you are the kind of person who keeps hitting the Remind Me Later button every time, consider using something like Ninite (https://ninite.com) to automate the installation (and subsequent update) process for your 3rd party programs.

Alternatively, you might want to consider using AppGet (https://appget.net/), Patch My PC Updater (https://patchmypc.com/home-updater-overview) or Npackd (https://npackd.appspot.com/) These are slightly different from Ninite but essentially serve the same purpose.

Change all your passwords on a regular basis, say every three months and, wherever possible, enable 2FA (Two-Factor Authentication) to ensure better security of the data on your system.

ADVANCED (3 points)

It is difficult to keep programs from accessing the various parts of your hard-disk once installed. Programs executed with administrative-level access can read (almost) everything on your hard-disk. Thankfully, there are a few ways to prevent your personal data from getting leaked in this manner.

[QR Code: https://rubica.com/wp-content/uploads/2019/02/Rubica-Report-Cyber-Crime-Privacy-Risks-in-Free-Mobile-Kids-Apps.pdf]

Why Doesn't Someone Do Something, Then?

In 2012, Google introduced a service codenamed Bouncer that provides automated scanning of apps submitted to the Play Store before making them available for download. Google Bouncer analyzes apps for any signs of hidden, malicious behavior and prevents suspicious apps from appearing on the market.

Info

Google Bouncer isn't a perfect service and some malware might still make it through the cracks. For example, in August 2019, an app called Radio Balouch found its way onto the Google Play Store, despite the fact that it contained the open-source spyware called AhMyth. Similarly, researchers from Kaspersky Lab revealed that the popular app CamScanner was also carrying malware, prompting immediate removal from the Google Play Store.

This doesn't mean that Google Bouncer doesn't work; it only means that no system is perfect and some malicious apps might still manage to slip through the cracks.

Apple has a separate team that analyzes each and every app that goes on to the Apple iTunes store. All apps in the official Apple ecosystem are thoroughly tested and vetted before being released to the general public.

Note that both Android users with rooted devices or Apple users with jailbroken devices are considered to be under tremendous risk of malware infection. Such users are probably likely to install apps from random unknown sources, which may further increase the severity of a malware infection.

Sandboxing

If we imagine your system to be your house, then programs are the guests that you invite to your house. Now, if a guest seems shady , wouldn't it be nice if you could hide certain parts and elements of the house from such a guest? Or construct a virtual house of sorts for the guests to visit before you invite them to your actual house?

Well, that's what sandboxing does. A sandbox is an area of your system that is isolated from the rest of your system. Programs installed in a sandbox are allowed to access only the resources available to the sandbox. Therefore, it makes sense to install any new programs within a sandbox to test them out before installing them on your system.

Sandboxing can be accomplished in a couple of ways:

Using a virtual machine: A VM is an operating system installed within an operating system. The guest OS uses the same resources as the host, but all processes and operations on the guest OS are completely isolated from the host.

Using a sandboxing software: A sandboxing software is akin to a virtual machine in the sense that it creates a mini-VM of sorts. However, sandboxing software usually restricts itself to isolating applications and processes, rather than providing an entirely alternative system experience. The most popular sandboxing applications are Sandboxie or Shade.

Sandboxed applications may feel slower than un-sandboxed applications because the programs and processes are filtered through an additional layer of security. However, my opinion is that any difference in speed or performance is definitely worth the additional security that sandboxing programs provide.

How can I prevent malware attacks in the future?

The easiest way to prevent malware attacks is to install a good antivirus/antimalware app that will do the job for you, but we strongly recommend that you also comprehensively review your browsing habits.

Are you the kind of person who believes that you are actually the millionth visitor to a website? Are you the kind of person who thinks random websites legitimately give away expensive gadgets for cheap, or even free? Are you the kind of person who gladly shares their contact details with all websites that ask for it? If you answered yes to any of these questions, then your troubles go way beyond the scope of this book. You desperately need what is called "Basic Awareness while Browsing the Internet."

For those of you in a hurry, here's the short version of it:

If it makes you think Wow! I am so lucky! or Did I participate in that? or something along those lines, it is almost definitely a scam. Do NOT fall for it.

As a rule of thumb, do NOT share your mobile number or your email address with anyone. If you absolutely must, maintain a separate number and email address to give out in such situations.

If the application being installed is named differently from what you clicked, or requires elevated, administrator privileges, or requires you to install something unrelated first, ABORT the installation right away.

The cardinal rule to prevent malware infections (which is also applicable to browsing the internet, in general) can be boiled down to three simple words:

"TRUST, BUT VERIFY."

File encryption

If sandboxing is akin to hiding your house from shady guests, file-encryption can be called 'locking' your valuables in a safe [4] to prevent 'shady' guests from accessing them freely. Specifically, if you can't (or prefer not to) restrict programs from accessing your data, you might want to consider restricting your data from being accessed by programs by using good file-encryption software.

There are several files, folder, and even disk encryption programs that are available for various operating systems, ranging from completely free and open-source (FOSS) to completely proprietary and premium. Most operating systems these days even provide (admittedly somewhat limited) file encryption capabilities out of the box. The table is given below lists some well-known file encryption programs that you might want to consider installing on your desktop:

Sandboxing

When you install an app on your Android device, it is copied to the system partition (a.k.a. internal storage) and allocated a folder that can be accessed only by the app. However, the app may choose to store some data on the external storage, which is the partition accessible to everyone —user, as well as other apps.

The problem is, the Android external storage isn't sandboxed, that is, apps that have been granted permissions to read and write to external storage can read any and every file on your external storage. What this means is data can be freely shared between different apps when it is stored on the external storage of your device.

That means, if you happen to download sensitive information, such as your bank statement from your banking app and store it in the Downloads folder in your external storage, any app with access to that folder can access and read that file without your explicit permission.

Info

External storage typically used to refer to removable storage in previous Android versions, but in recent versions, it has taken on the rather vague meaning of that partition of phone storage, which is accessible to apps for storing and retrieving information that can be copied to and from the phone to other external devices such as USB, PC, and more. Typically, this is also referred to as the 'data' partition on your phone.

	Win	MacOS	Linux	License	Pricing Model
FileVault	×	(inbuilt)	×	Proprietary	Free
BitLocker	(inbuilt[5])	×	×	Proprietary	Free[6]
GnuPG	✓	✓	✓	Open Source	Free
VeraCrypt	✓	✓	✓	Open Source	Free
AxCrypt	✓	×	×	Proprietary	Freemium
Concealer	×	✓	×	Proprietary	Paid
Folder Lock	✓	×	×	Proprietary	Freemium

Table 8.1: A comparison of commonly available encryption software for various operating systems

These are just a few of the several encryption programs available for your system. Not all of these programs perform the same functions. Some encrypt files, some encrypt folders, some encrypt entire disks, and some do two or more of those three things. Before you install any of them, I strongly recommend you read up on what each one of them does and whether it fits your specific requirements.

Permissions

In its early days, Android adopted a very relaxed permissions model , that is, apps were allowed to ask for any permission from the user. This led to a bunch of apps misusing and abusing the liberal permissions model [1] , until Google was forced to crack down on such unethical behavior.

Until Android v6.0 Marshmallow, these permissions were granted to the apps at the time of installation. However, starting from Android v6.0 Marshmallow, runtime permissions were introduced, which allowed users the ability to grant or deny permissions when the app was actually being used. Runtime simply means that the app needs to ask for permission when it is 'run' by the user, and not just at the time of installation.

Moreover, the internet permission is no longer classified as a dangerous permission since Android v6.0 Marshmallow, that is, all apps are now allowed to use your device's internet connection, if they wish to do so. This means, an app with a set of rogue permissions can collect data and share it silently with third-parties without your explicit permission to do so. For example, a malicious app with READ/WRITE EXTERNAL STORAGE permission can silently upload all files stored on your external storage to a remote server without your knowledge. If your bank statement happens to be in the Downloads folder, well, bad luck!

Additionally, apps do NOT need to be given all the permissions that they ask for. You are free to grant certain permissions, and deny other permissions to the app. If the app is well-designed and well-developed, it can handle this loss of permission properly, without crashing. If the app does crash, then it is probably a sign that you might want to look for an alternative.

Why deny permissions, you ask? Well, because most apps will try and collect as much data about you, as they can. For example, the Google app requests the location permission to ensure that it can relay back accurate location information to Google servers for the Find My Phone feature. However, granting the location permission to the Google app means that it can be used by the Google app to provide you location-relevant search results.

Info

You can't run and you can't hide…

Even if you deny location permissions to the Google app, it will still try and narrow your location based on the IP address, recent locations, or Location History. In some cases, Google has been known to utilize telemetry data, such as Wi-Fi and cellular network information, to serve you location-aware results when you search on the app. Don't believe me? Try searching for "Chinese Restaurants" on your Google Search app.

Notice how Google immediately tries to identify your location and provides you location-aware results at the very top.

Now, some of you may argue that it is a trade-off for being able to know where your phone is all the time. However, it leaves the door open for multiple malicious actors to leverage this through nefarious means.

System restore

The final option in this set of recommendations is the option to restore your system to a previous state. System restore is the ability to revert the system back to the state, it was at an earlier time; for example, before a certain program was installed. This comes in very handy if you accidentally install a program that somehow messes up your system.

In Windows, open the System Protection tab in System Properties , which can be accessed by either by:

Right-clicking the My Computer icon OR

Clicking System Infoon the left under Related Settings in Settings | System | About

macOS doesn't have an identical equivalent of system restore in Windows. The closest option available is Time Machine that works by making backups of files to an external storage device. Note that Time Machine does not back up your entire OS the way System Restore does. However, you can use Migration Assistant to restore older backups from Time Machine after a reinstall.

Similar to MacOS, Linux doesn't have a System Restore kind of functionality, but there are a few third-party apps (for example,TimeShift, CronoPete, Back In Time, and many more) that can help you by taking snapshots of your system and restoring snapshots as and when needed.

RohitRecommends

When it comes to smartphone apps, I believe in the motto Less is more.

The fewer apps you have on your smartphone, the lesser the chances of your information being leaked to various third-parties. It also reduces the available attack surface for adversaries. However, this is not easy to achieve, given that we live in a world in which the number of apps and the number of malicious actors keep growing, every minute of every day.

Bloatware removal

I have observed that people usually don't bother investigating their desktop PCs and laptops for bloatware. Most users work under the assumption that, If it already exists on the machine, then it must be required. As we have already seen in the previous sections, this is not always true and, in some cases, the exact opposite of the actual truth.

Remember the rules of data-sharing, specifically, rule no. 3?

"If the data is encrypted, but not in your control, then it might be secure, but it is not private."

Clearly, in this case, you are better off removing all the bloatware from your desktop OS installation. Here are a few recommended steps to help you get rid of as much bloatware from your system and keep your system as lean as possible.

Bloatware

Here are a few methods to quickly and cleanly identify (and possibly get rid of) unnecessary bloatware on your smartphones and tablets.

Windows 10

Typically, most manufacturers provide a recovery method built-in with their customized version of the Windows 10 OS. Dell, for example, has something called SupportAssist OS recovery baked into most of the Windows 10 PCs, tablets and laptops that it sells.

However, if you're looking to remove manufacturer-branded utilities from your system, this is (obviously) counter-intuitive. Instead, you can try one of the following methods.

BASIC: (1 point)

Uninstall programs through the Settings or through Control Panel in Windows. Most bloatware is actually legitimate programs installed but without explicit user consent. If you find a program that you don't want, open the Settings app and then click on Apps . In the section titled Apps and Features find the program that you don't want and click on it. Click the button named Uninstall and Windows will remove it from your system.

If you prefer to use the Control Panel instead, look for the icon that says Programs & Features and click (or double-click) to open it. Find the program you wish to uninstall, click on it, and then click on the Uninstall text/button that appears in the header.

On Android

(Overheard somewhere…)

Q: How do you get rid of bloatware on Android?

A: With great difficulty…

Jokes aside, since bloatware is directly influenced by the phone manufacturers, they have very little incentive to provide proper uninstallation methods. Often, you'll find that there is no uninstall option for these apps—you can only Force Stop them or Disable them, or in some cases, Uninstall Updates . None of these options removes the apps completely from your system.

INTERMEDIATE: (2 points)

If you've been using your PC for a while and have installed programs that you would rather not install all over again, then consider using a persistent uninstaller program such as the ones developed by IOBit, Revo Uninstaller, or such. Scan the QR code given alongside to check out a (somewhat) comprehensive list of various uninstaller programs.

BASIC: (1 point)

Open the Settings app on your phone and scroll down to the Apps section. Click on it to open it and select the option that allows you to view all the apps on your system. One-by-one, click on each app and ask yourself the question, "Do I really *need* this app? Or can I do without it? Can I access the same functionality using a browser?" If the answer is not an emphatic, "I NEED THIS APP!", then the app doesn't need to be on your phone and can probably go:

[QR Code: https://www.lifewire.com/free-uninstaller-programs-2625188]

Remember, you must always make a system restore point before attempting to uninstall any bloatware -- especially if you have a good reason to believe that uninstalling specific bloatware might destabilize your system! If things do not go as expected, you will at least have the option of rolling back to the earlier restore point.

First, you need to identify the bloatware you wish to remove. To do this, open your Settings app and click on Apps . In Windows 7, this feature is called Programs & Features and it can be found in the Control Panel [7] .

Search (or scan through the list, if you're on Windows 7) and make a note of the apps that are irrelevant to your daily usage. Click on the app to select it, and then click Uninstall to remove it from your system.

Alternately, you can use third-party decrapification tools to help you remove unnecessary software from your PC. These decrapification tools look for common bloatware installed on your system and can often be run as portable programs, that is, you can run them off a flash drive, without needing to install them.

Some popular, trusted decrapification tools that you can use are:

The PC Decrapifier

Should I Remove It?

Slim Computer

A quick search on the internet will provide you with the relevant URLs for downloading and installing each one of them.

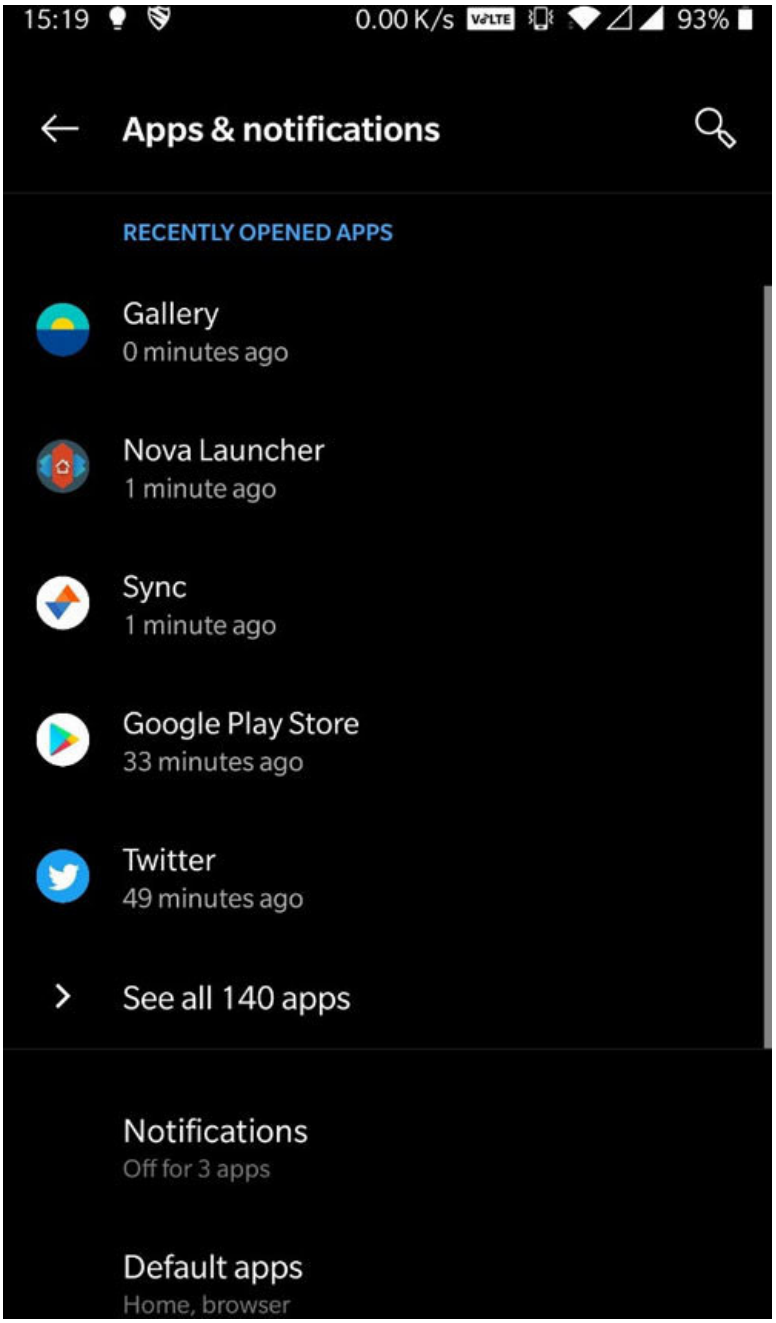


Figure 5.1: The 'Apps & notifications' section in the "Settings" app as seen on a OnePlus 5, running OxygenOS version 9.0.9

For example, the shopping apps you have installed on your phone get used only once in a blue moon. However, you can be sure that they are constantly sending data on your phone usage habits and analyzing your usage patterns.

ADVANCED (3 points)

One of the easiest ways to ensure minimal bloatware on a new PC is to perform a clean install. This is definitely recommended for all new desktop PCs or laptops that you may have newly purchased from a manufacturer.

A clean install (typically recommended for Windows-based PCs) involves reinstalling your OS from scratch. There are two different clean-install methods:

Windows Recovery: Open Settings| Update & Security and click on the section titled Recovery in the sidebar. Click the Get Started button and choose the option that says Remove Everything . This is akin to factory-resetting your Windows 10 PC, which means all your manufacturer-branded utilities are likely to return, once this process finishes.

Windows 10 installation Media: Download the Windows 10 installation media from the official Microsoft website and run it on the system you wish to install. If you are prompted to Keep personal files and apps or Keep personal files only, or Nothing, choose Nothing .

Make sure you have backed up all your important documents, exported any important data, and saved all important files to at least two different locations that are not on your machine BEFORE you attempt this step. System Restore points will NOT help in this case.

Understand that you WILL lose all your data, all your apps, all your documents -- everything -- if you perform a clean install on your machine.

"Un-uninstallable"applications

If you come across an application that can't be uninstalled, it could mean one of two things:

The application is necessary for core OS functionality and is marked as a system tool

The application is NOT necessary for core OS functionality BUT is marked as a system tool

The following section is meant merely for your information and is not to be treated as a recommendation of any kind. I recommend that you consult with an expert before you proceed along this path.

INTERMEDIATE: (2 points)

Once you have identified the bloatware app you want to remove, you can either uninstall the app or disable it.

Uninstall: To uninstall an app, long press the app icon either in the app drawer or on the home screen, then click on (or drag the app to) the trash can icon to uninstall it. Alternatively, you can go to Settings | Manage Apps and scroll down to the app, tap on its name, and then click on Uninstall .

Disable: Some apps (such as the apps provided by Google Mobile Services) only allow you to disable them rather than uninstall. Clicking Disable is somewhat similar to uninstalling, except the app isn't completely removed from your phone—you can re-enable the app at a later date, if you wish.

Google provides detailed instructions on how to 'disable' system apps. Scan the QR code given alongside this section to open the official Google Support page that details this procedure.

EXPERT (5 points)

Modern versions of Windows, (that is, versions of Windows 8 and above) come pre-installed with a bunch of applications that don't serve much purpose other than cluttering up your system and infringing on your privacy. These applications are also marked as system applications which means that they cannot be uninstalled using the method outlined in the previous section.

Fortunately, there exist multiple free, trusted, third-party tools such as O&O App Buster and Windows X App Remover . These tools [8] are aimed at specifically uninstalling such pre-installed Microsoft applications. Furthermore, since these tools are portable, that is, they don't need to be installed, you can download and run them off a flash drive if you so wish.

Important!!

ONCE AGAIN, I DO NOT RECOMMEND DOING THIS WITHOUT PROPER SUPERVISION BY AN EXPERT!!

Be very careful with what you choose to remove and always, ALWAYS make a system restore point before you remove any un-uninstallable applications. If things go south, you can always restore your system to the system restore point and prevent yourself a huge headache.

Also, conduct the necessary research (or, at least a quick search on the internet) to ensure that the software you are trying to uninstall is, indeed, bloatware. Some packages might look suspicious (for example, Microsoft .NET Redistributable packs) but are actually essential because other important programs on your device may be dependent on them.

[QR code: https://support.google.com/googleplay/answer/2521768?hl=en]

Apple (macOS)

ADVANCED: (3 points)

Important!!

The actions described in this section require your Android phone to be rooted. If you have NOT rooted your device, do NOT read any further—skip this section and head straight to the next one!

A quick search of the keyword bloatware on the Google Play Store reveals that there are many apps that will help you uninstall bloatware from your rooted device—many of them made by reputed companies and developers.

However, the best app and the one that many, many experts on the internet will recommend without hesitation is Titanium Backup Pro. You'll need the full version with the Pro license to use its best features. It costs 400 INR (as of September 2019) on the Google Play Store, but it is worth every rupee.

Important!!

NEVER EVER MAKE ANY CHANGES TO YOUR PHONE WITHOUT CREATING A FULL BACKUP FIRST!

Install Titanium Backup Free, and then install the companion license app, i.e., the Pro key. Launch it and grant it superuser permissions when it prompts you.

You can now decide whether you want to Backup, Freeze, or Uninstall the offending bloatware apps. To do this, you need to open the Backup/Restore tab, scroll down, and tap on the name of the app. A dialog box opens with details about previous backups and displays the three actions: Backup, Freeze , and Uninstall .

1) Use the Backup button first to create a backup of the app, in case something goes wrong.

2) If you want the app to still be available in case you change your mind, tap the Freeze button at the top.

3) If you are sure you want the app to absolutely disappear, tap the Uninstall button instead.

Frozen apps can be defrosted in Titanium Backup Pro by repeating the same steps as above, and clicking Defrost instead of Freeze . Uninstalled applications need to be re-installed or can be recovered.

Alternatively, on rooted phones, you can also use a regular root-aware file manager app, such as Root File Explorer Pro, to carry out bulk deletions of bloatware apps. Be careful, though, you are very likely to break apps if you don't know what you are doing.

BASIC: (1 point)

For Apple devices (that is, devices that run macOS) as their primary operating system, bloatware isn't much of a problem because Apple systems don't ship with much bloatware (except stuff like GarageBand, Movie Maker, and many more, which you may not need) and if you see a program or a utility you don't like, you can simply uninstall it as follows:

Open the Launchpad, that is, the spaceship/rocket-shaped icon in your dock to open a list of currently installed apps.

Find the app you want to remove and click and hold the app icon. An x will appear on the top left of the icon, and the icon will start shaking.

Click the x and click Delete when prompted.

That's it. You're done.

EXPERT: (5 points)

Important!!

The actions described in this section require your Android phone to be rooted. If you have NOT rooted your device, do NOT read any further—skip this section and head straight to the next one!

Buckle up, because this involves connecting your phone to the PC and making changes to it using the Android Debug Bridge (ADB). A detailed guide can be found on XDA forums here:

Linux

Linux machines usually don't ship with bloatware. That said, if you happen to come across any non-essential application or software that you don't need on your system, you can use your system's package manager software (either command line or GUI) to uninstall that particular software and its various dependencies.

[QR Code: https://www.xda-developers.com/disable-system-app-bloatware-android/]

To sum it up quickly, here's what you'll be doing:

Install the ADB drivers, download the Android SDK platform tools and unzip them to a convenient directory of your choice, and connect your phone to the PC.

Use an app like App Inspector or drill down in App Info to figure out the package name of the bloatware app that you want to remove from your phone. For example, the package name for the Google Chrome browser is com.android.chrome

Open a Command Prompt or PowerShell window (or a Terminal window, if you are a Mac user) in the directory with the ADB binary and enter the following command depending on your OS:

Windows Command Prompt:

adb shell pm disable-user --user 0

Windows PowerShell:

.\adb shell pm disable-user --user 0

Mac/Linux Terminal [2] :

./adb shell pm disable-user --user 0

Note

There are various apps available on the Google Play Store that claim to disable/uninstall all kinds of bloatware and malware, even on unrooted phones. While a few of them may actually perform as advertised, most of them are themselves suspect. I strongly recommend that you consult with someone who is knowledgeable about Android phones before you install any such apps!

Removing Bloatware on Apple Devices

Getting rid of bloatware on Apple iPhones is a three-step process:

Switch on your iPhone.

Press and hold the app that you want to remove or delete—hold till all the apps on the screen start shaking.

Tap on the red x button to delete the app.

That's it, you're done!

BASIC: (1 point)

For example, suppose you want to uninstall jabber (a messenger application) from your default Ubuntu or Linux Mint install. All you have to do is open the Software Center, search for a package named Jabber and click uninstall. Alternatively, just run the following command:

$ sudo apt-get remove jabber

And enter the root password, and the application will be uninstalled. Simple, isn't it?

Malware

In the event that your phone is infected with malware, you should take immediate steps to identify and remove it from your system.

Security software

Regardless of how secure you think your system is, installing good security software is always recommended. At the very least, setting up a good firewall and an antivirus should be considered a bare minimum for every desktop system that you use.

I'll outline a few examples of how to get the best out of your security software and the usage hygiene you need to implement to make that happen. Remember, security is not an end-product -- it is a mentality that you need to cultivate and implement.

Tips

I strongly recommend NOT using any 'unknown' systems, especially if they don't use at least a firewall and an antivirus, e.g. computers at a cyber-café. Chances are, you might end up unknowingly leaking crucial personal data (such as your netbanking credentials) to an eavesdropping malicious actor.

If you absolutely must log in to an unknown system, make sure that you immediately change the credentials from a 'known' computer in order to mitigate any potential damages arising from the act.

BASIC: (1 point)

Uninstalling suspicious apps: Open your Settings app and navigate to the list of Installed Apps . See if you can identify any apps that you did not (consciously) choose to install and remove them immediately. If you are not sure about an app that is installed on your device, search for relevant details on the internet.

Third-party tools: You can also use one of the many antivirus/antimalware apps available in the Play Store. Some of the more popular ones are Security Master, Bitdefender, AVG, Malwarebytes, Quick Heal – again, the internet is a rich source of information for choosing the right one for your device.

Windows 10

Simply put, due to the massive numbers of attack vectors present in the wild, every Windows 10 system needs to have security software installed and active.

Let's look at the various options for both kinds of security software (firewalls and antivirus/anti-malware programs) that you have at your disposal for your Windows 10 system.

ADVANCED: (3 points)

Android safe mode: If, for some reason, you are unable to uninstall an app, reboot your Android device to Safe Mode . Go into your Settings app, open the list of installed apps, and remove any applications that might seem suspicious or malicious.

Remember, if your device has been infected with malware, your data may have been compromised. I strongly recommend that you change all your important credentials immediately, that is, change the passwords to your Google account(s), your banking credentials, and any other accounts that you believe may be affected.

Finally, if you still keep seeing ads and junk offers on your device, then you probably will need to factory reset your phone . Should you need to do this, I have TWO recommendations:

Backup all your data—your photos, documents, contacts, text messages, and many more—to an external storage device.

Instead of restoring your apps from the backup, reinstall them from the Google Play Store after the reset. You can use this as an opportunity to re-evaluate your app needs and only install apps as and when you need them.

I recommend the same for users who have rooted their Android devices, or jailbroken their iPhones.

Firewalls

Sandboxing

While most apps ensure that no sensitive personal information is allowed to leak out of internal storage, there may be instances where sensitive data might accidentally end up in the universally accessible external storage on your device.

For instance, you may download a bank statement and store it in your Downloads folder. Or you may download secret correspondence and save it in a text file in some folder on external storage. In both these cases, the downloaded files are accessible to you and also to any app that has the READ/WRITE EXTERNAL STORAGE permission.

BASIC: (1 point)

All Windows 10 installations automatically come with an inbuilt security solution named Windows Defender, right out of the box. Windows Defender is a suite consisting of a firewall and an antivirus with malware-detection capabilities.

The Windows Defender Firewall is a part of the Windows Security app which can be accessed through the Start menu, or by opening Settings | Updates & Security | Windows Security and clicking on the button titled Open Windows Security .

Open the Firewall & network protection section from the sidebar and ensure that the firewall is on for all three kinds of networks, that is, Domain Network, Private Network, and Public Network.

If, instead, you see a button named Turn On , click the button to activate it.

BASIC: (1 point)

Prevention is always better than cure, so I strongly recommend that you do NOT download or store sensitive information to any folder on your external storage .

In case you do end up downloading sensitive information to your external storage, well, good luck. There is no way to know when the file was last accessed or which app accessed it. The most you can do is check which of your apps has been given the READ/WRITE EXTERNAL STORAGE permission and hope that none of them are malicious.

INTERMEDIATE: (2 points)

If for some reason, you do not trust Windows Defender, you also have the option of installing your preferred third-party firewall. There are several free and paid options you can choose from, ranging from popular names such as Comodo, Norton, and ZoneAlarm to lesser-known but superb options such as TinyWall, GlassWire, and PeerBlock.

Permissions

Even though the user now has greater control on the permissions being granted to each app, they are still vulnerable to the visual fatigue phenomenon—users grant their apps all the requested permissions, often blindly and mechanically. Apps use these permissions to collect and share all kinds of user metadata with their remote servers—we even showed you an example at the very beginning of the book, remember?

Antivirus & Anti-malware

BASIC: (1 points)

Here are my recommendations to keep those permission-hungry apps under control:

Carefully evaluate every permission request made by an app instead of blindly clicking Allow every time the app prompts you to grant some permission.

Don't hesitate at all if you need to deny permissions to apps. Well-designed apps will usually explain why they need the permission.

Delete any apps that don't explain why they are asking for out-of-scope permissions, for example, a Flashlight app shouldn't be asking for location permissions at all.

Review every permission that you have given an app by opening Settings| Installed Apps| Permissions .

As for Google's shady behavior with location permissions, well, here are a few different ways to deal with Google's overall disregard of the privacy of your personal data.

Use a privacy-focused search engine app such as DuckDuckGo or StartPage, instead of the Google app on your phone for searches. Use a completely separate Find my Phone app to circumvent Google's unwanted sharing of location permissions.

BASIC: (1 point)

The Windows Security app also has a section in the sidebar titled Virus & threat protection . Click on it and ensure that the text under the heading Virus & threat protection settings says no action needed. If, instead, you see a button named Turn On, click the button to activate it.

Note

The malware detection service (also referred to as threat-protection in the Windows Security app) can be a little unreliable at times. I recommend installing at least a competent anti-malware program (such as MalwareBytes Anti-Malware or SpyBot Search & Destroy) and using it in conjunction with Windows Defender.

INTERMEDIATE: (2 points)

Use a privacy-aware browser such as Firefox Focus, Brave, or Epic, and navigate to the duckduckgo.com webpage or the startpage.com webpage

to execute your searches. Startpage, for instance, is built by a Dutch company and the search engine queries Google for results on your behalf. It also provides the Anonymous View feature to view the results anonymously.

INTERMEDIATE: (2 points)

Similar to firewalls, if you want something more than the inbuilt Windows Defender, then you can install your preferred third-party antivirus software. In fact, there are tons of third-party antivirus programs available for your Windows 10 system, with both paid and free versions that you can download and install. Among the most popular are BitDefender, Avast, Avira, ESET, Kaspersky, QuickHeal, and many more.

Some of these programs may even provide multiple internet security solutions, that is, they protect against viruses, malware, intrusions, scamming & phishing attempts, and many more, for a fee, that is, paid version.

Note

Simply having a good firewall and antivirus program on your system isn't enough.

Sure, firewalls and intrusion prevention systems can identify and block several threats, but, sometimes, some threats can slip through the cracks. Sometimes, malware can lie dormant until certain conditions are met and then suddenly become active. Scanning your system regularly for infections and threats helps mitigate some of these risks and may help prevent untimely loss of valuable data.

ADVANCED: (3 points)

Use a VPN to add another layer of security and/or anonymity to your browsing. A VPN or Virtual Private Network is an additional layer between you and the search engine, which allows you to mask your real IP address. Using a VPN is akin to playing Chinese Whispers—only more efficiently and without losing any information in the process.

macOS and Linux

You'll hear a lot of people claiming that both macOS and Linux are malware-resistant, that is, there is very little chance of them getting infected by a virus or malware.

This is not entirely untrue. Linux and macOS insist on user accounts that do not have administrator (or root) level access. Thus, any applications installed for a user are installed specifically for that user, and the installer is typically not given system-wide permissions. This level of compartmentalization ensures that any malicious programs do not get to infect the whole system. However, they may still act as carriers for viruses, that is, carry potentially malicious executable (a.k.a. EXE files) that might infect other Windows PCs.

Therefore, one of the arguments for running antivirus software on your macOS or Linux system is to ensure that the other Windows systems on your network (if any) do not get infected!

So, let's look at some options for firewalls and antivirus on macOS and Linux systems

Conclusion

Smartphone apps may have originally started off as curiosities, but they are now very much necessities. You cannot imagine travelling without Google Maps any more. You cannot imagine NOT having access to your email on the go. You cannot imagine not being able to exchange messages instantaneously with your loved ones. You cannot imagine NOT capturing a nice moment and sharing it with your friends and family.

In other words, smartphone apps are what make the smartphone, well, smart. Therefore, it stands to reason that they must be treated with utmost care and caution. You should never install apps of unknown origin. Sure, app stores usually take care to prevent malicious apps from reaching you, but, sometimes, carefully-crafted malicious apps may slip through the cracks. You still need to be the last line of defense on your smartphone.

It helps if you think of smartphone apps as a house that someone wants to give away for free. If someone made you such an offer, I'm sure your first question would be, What's the catch?

You need to ask the same question whenever you are about to install a free app. I suspect you are likely to find answers that you might not like.

---

[1] Remember the Flashlight app that needed location permissions? Yeah, that.

[2] Note the different types of ‘slash’ used for Windows PowerShell and MacOS—Windows uses the backslash, while MacOS uses a forward slash.

BASIC: (1 point)

Firewalls

macOScomes with an inbuilt firewall which is turned off by default. To enable this, open the Launchpad and click on System Preferences . In the Firewall tab, select the grey radio button titled Firewall: Off to turn on the firewall. The change will be signified by the grey radio button turning green.

According to the website AverageLinuxUser.com, you do not need [a firewall], but it is better to have [one]. The most commonly used Linux systems (for example, Ubuntu) have a firewall included in the kernel, which can be configured using the iptables package, but the interface is disabled by default. You can install gufw (short for Graphical UFW or Graphical Uncomplicated Firewall) to configure rulesets as per your requirements.

[QR Code: https://averagelinuxuser.com/linux-firewall/]

Chapter 6

Smart Devices and IoT

Antivirus and anti-malware

macOSdoes not have antivirus software built into it, be the default. macOSdoes have a feature called GateKeeper. GateKeeper is a service/feature that prevents you from installing apps that are not from the Mac App Store and/or from identified developers. macOS also has File Quarantine, built-in anti-Malware protection, which is very similar to the SmartScreen feature deployed by Windows. It checks downloaded files against known malware definition signatures and warns you if a match is found. However, compared to Windows Defender, both these alternatives are fairly rudimentary.

Linux systems do not have any antivirus software installed by default or built into the system because they genuinely do not need it. However, there are several third-party applications that you can download and install, details of which I'll provide in the next section.

Introduction

When Steve Jobs demo-ed the first iPhone, the whole world was taken by storm and, right then and there, everyone knew two things for certain:

The market would soon be filled with BIGGER 'smart' devices.

The market would soon be filled with SMALLER 'smart' devices.

As of August 2019, we can safely say that BOTH these assumptions were right.

Since that historic day in 2007 (29th June 2007, to be exact) there has been constant innovation in the world of smart devices -- sometimes to the extent where one is forced to ask the question,"but why does THIS device need to be smart?"

Regardless, it must be noted that we live in a world where smart devices have now become extremely common and wide-ranging. These days, we see tiny smart devices, from fitness bands to mini-cameras, and we also see huge smart devices such as wall-to-wall smart TVs and refrigerators.

A wide variety of smart-devices is available for consumer usage, ranging from simple door locks without keys, to the more complex smart TVs and refrigerators, to the really quirky smart diapers, water bottles, hairbrushes, pregnancy test kit, candles or even sex toys!

Info

As you can see that not all smart devices are necessary, or even useful! Check out the

ADVANCED (3 points)

There are several third-party alternative firewalls, antivirus, and anti-malware software, offering several additional features that you can install on your macOS and Linux systems. Note that the list provided below was constructed in September 2019 and it may have significantly changed since then.

You can always find an updated list at the companion website for this book, that is, https://privacy.clinic . Simply scan the QR code given alongside this paragraph to open the home page on Privacy Clinic in your phone browser, right now.

Tumblr blog, " We put a chip in it!" at https://weputachipinit.tumblr.com/ for some crazy examples of 'smart' tools and devices! Although many of these devices have now disappeared from the market, the very fact that they existed at some point is a good indicator of the kind of 'smartness' we have now come to expect from tools and utilities we use daily.

Note that smart devices do not necessarily need:

To be a handheld, portable, or wearable: They may be fixed in position and still be able to fulfil both the above criteria, for example, a smart refrigerator or a smart TV.

To have a touchscreen for interactivity: They may use other kinds of input. For example, smart speakers such as Alexa, Google Home, and many morerely on voice commands.

Some smart devices:

May use auxiliary devices for extended interactivity; for example, smart bands typically come with a companion app that connects with the smart band to exchange information with the app.

May be intended primarily for data collection and only provide rudimentary on-device interactivity, for example, the Nest thermostat by Google.

May exhibit some degree of artificial intelligence or machine learning by analyzing basic user behavior and compiling recommendations or suggestions for the user based on these analyses, for example, a smart speaker such as Amazon's Echo or Google Home.

So, what makes a smart device, smart ? I'd say that the two key features of smart devices are interactivity and autonomy:

Interactivity: Smart devices typically provide an interface for the user to issue various commands for operating them in a certain manner.

Autonomy: At the same time, smart devices have features that allow it to carry out certain automated tasks unsupervised.

For example, smartphones allow for a wide range of interactions and, at the same time, also execute automatic background processes that do not require any user input whatsoever.

These devices usually employ different wireless protocols such as Bluetooth, Wi-Fi, NFC, and many more, to connect with each other. They may also communicate with remote servers to accomplish more powerful and nuanced processing of data collected in the course of their usage. This ability to connect to other (similar) devices and operate (somewhat) autonomously is often commonly referred to as the Internet of Things (IoT).

[QR Code: https://privacy.clinic/]

Firewalls

While the default macOS firewall does a pretty good job of monitoring your internet traffic, those of you who wish for something more detailed might want to consider installing one of the following on your macOS system:

"Hands Off!" by One Periodic

"Little Snitch"

Murus

Radio Silence

Avast Internet Security

Most of these firewalls are available in both free AND premium versions. The free versions usually offer just the basic firewall functionality with a better interface than the inbuilt firewall but, in most cases, the premium versions (typically) offer slightly enhanced features. Some providers such as Avast may even provide the firewall, antivirus and anti-malware features combined in one single package.

Also, please note that this list is not exhaustive -- there are several other options that you might want to consider. For the latest recommendations, check out the QR code given at the beginning of this section.

The Internet of Things (IoT)

The most common example of IoT that is usually given is that of an automated smart home -- think Tom Cruise's character's home in Minority Report. Installing IoT-enabled devices provides Tom's character in the movie the ability to control several home utilities such as the entrance lock, lights, entertainment system, refrigerator, by issuing simple voice commands and/or gestures.

In the simplest terms, the IoT is a system of interconnected devices (each with its own unique identifier ID) that can communicate without requiring any human intervention whatsoever.

One of the earliest examples of an IoT-enabled device dates back to as early as 1982 when a vending machine installed at Carnegie Mellon University was modified to be able to report its inventory and temperature details on the contents of its freezer:

Antivirus and anti-malware

Similar to firewalls, there are several free (and premium) antivirus & anti-malware software programs that can be downloaded for macOS. Most of the well-known antivirus companies offer both free and premium antivirus solutions for both macOS and Linux-based systems. Some options you might want to consider for your macOS system are:

Avast Internet Security

Intego Mac Internet Security X9

Bitdefender

Sophos Home

Clam XAV

Malwarebytes Anti-malware

Among others, whereas for Linux-based systems, you might want to consider installing one of the below options:

Clam AV

Comodo Antivirus

Sophos Antivirus

ClamTK

Chkrootkit

Rootkit Hunter

As mentioned earlier, a list of the current most popular options will always be made available at privacy.clinic, the companion website to this book. Scan the QR code given alongside this paragraph to view the companion website in your browser.

[QR Code: https://privacy.clinic/]

Figure 6.1: The ‘internet-connected’ vending machine installed at Carnegie Mellon University. (Image credits: https://www.engineersrule.com/how-a-coke-machine-and-the-industrial-internet-of-things-can-give-birth-to-a-planetary-computer/)

You can read the fascinating history of how this vending machine came to be on the official page of the Computer Science department of Carnegie-Mellon University, by visiting:

https://www.cs.cmu.edu/~coke/

Alternatively, scan the QR code given alongside to open the page in a browser on your device. Although this page is no longer updated, it has been made available for historical reasons and provides a fascinating insight into the early days of IoT -- much before the term, IoT was even coined.

Conclusion

Without a doubt, Windows is the target of choice for malicious actors and hackers looking to access data in all kinds of unauthorized manner. However, that shouldn't be taken to mean that macOS is the safer option, though. With the popularity of Apple devices increasing every day, macOS and iOS will soon become a viable target for malicious actors to develop potentially harmful malware.

Already, according to the 2018-19 security report from AV-TEST [PDF], the number of malware programs for macOS has almost tripled […] there were nearly 100,000 samples found that affect Macs in 2018.

Security vulnerabilities in IoT and smart devices

IoT devices have certainly come a long way since that simple vending machine and now find large-scale acceptance in our day-to-day life through several consumer-oriented applications such as smart thermostats, doorbells, locks, etc. and also through large-scale industrial applications in manufacturing, agriculture, and infrastructure development to name just a few.

The IoT can easily encode (that is, track and follow) between 50 to 100 trillion objects and it is expected that the world will have close to (or even more than) 200 million IoT devices by 2020.

As you may have realized by now, this behavior goes against the three fundamental rules of privacy that we have outlined earlier in the book. There have been multiple instances of vulnerabilities being discovered in various smart devices which were then subjected to subsequent exploitative attacks. The following section contains some of the more famous examples of IoT devices being breached:

[QR Code: https://www.av-test.org/fileadmin/pdf/security*report/AV-TEST*Security*Report*2018-2019.pdf]

Of the three operating systems we have been discussing, I would say that Linux offers the most security, privacy, and transparency due to its FOSS philosophy. The macOS, owing to various factors (market and non-market) probably takes second place, while Windows comes in a distant third on all counts.

However, if you were to rank them according to ease-of-use, macOS and Windows both rank higher than Linux. Linux also scores poorly in terms of user-friendliness of interfaces and overall design. Cost-wise, Linux systems win by a huge margin since Windows and macOS both required a paid license to run on your system.

The one thing that definitively sets Windows apart from the rest of the pack is the sheer number of (third-party) applications available for the OS. According to a post made on Windows Blogs (as linked via the QR code) in November 2018, there are over 35 million application titles with greater than 175 million application versions, and 16 million unique hardware/driver combinations. Just to present a comparison, Android and Apple only have a couple of million apps each on their App stores.

Strava

Strava is an app primarily aimed at athletes -- specifically runners and cyclists, and it shows the most popular routes for running and cycling. The Strava app can be synced with multiple smartphones, monitors, and fitness trackers, to record various performance metrics of its users.

[QR Code: https://blogs.windows.com/windowsexperience/2018/11/13/windows-10-quality-approach-for-a-complex-ecosystem/#LTW3DJvWw3d4cXb4.97]

All said and done, the one piece of advice I would definitely want you to take away from this chapter is this:

Always be aware of what programs are running on your system at ALL times.

If you find something suspicious or see something that you don't remember installing, ask the internet immediately! Honestly, spending a few moments to run a quick internet search on your preferred search engine is much better than spending hours to restore a system that has been overtaken by malware.

---

[1] Yeah, I'm explicitly saying that pirated software falls under the category of "Unauthorized software." I'll explain that in a bit.

[2] Applicable for all operating systems -- Windows, MacOS and Linux

[3] I'll tell you how to deal with browser plugins in a later chapter.

[4] Note, you can encrypt your files AND sandbox applications.

[5] Not available for Windows 10 Home version

[6] See above.

[7] The "Control Panel" is also available in the modern versions of Windows, i.e. Windows 8 & up. Simply search for Control Panel in your Start menu.

[8] I've chosen not to include QR codes that directly link to these tools, since they shouldn't be used on a whim. In any case, for the truly curious, they are merely an internet search away. Caveat Emptor!

In 2017, the Strava released a data visualization map, with more than 3 trillion individual GPS data points, that showed a heatmap of all activities

uploaded to Strava by its users. However, soon after the visualization map was made public, military analysts realized that it (the map) was detailed enough to inadvertently give away locations and movements of military personnel, who also happened to be users of Strava.

For more details, check: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Chapter 9

Desktops-Browsers

Smart TVs

A study by Consumer Reports in 2018 found that millions of smart TVs were susceptible to attacks by malicious actors. A malicious actor who gained control could turn up the volume, rapidly switch through channels, open disturbing content, and disconnect the TV from the Wi-Fi network. Thankfully, this specific vulnerability did not allow the malicious actor to extract any private information, or monitor what is being played on a smart TV. The QR code given alongside this paragraph links directly to the study published by consumer reports, in case you wish to read it for yourself.

Introduction

You must be wondering, Isn't a browser just another software application? Didn't we already discuss software applications in the previous chapter?

You see, if the operating system is the primary agent between the user and the internet, the browser is the interface through which the user accesses the internet. Browsers belong to a special class of software applications since they are often the user's first window to the internet. Therefore, in this chapter, I will be discussing browsers as an independent entity with a separate set of privacy implications.

[QRCode: https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/]

A specific exploit for Samsung's F-series smart TV was designed by the CIA jointly with MI5, in June 2014. It was called the Weeping Angel attack (released in the Vault 7 leaks by Wikileaks), and it allowed anyone with physical access to these Samsung Smart TVs to installing a malicious firmware. This malicious firmware would pretend to put your TV in a fake ‘off’ mode but would remain on and could record all the audio, and upload it when it was switched back ON. The QR code given alongside this paragraph will lead you to a page on Wikileaks describing the Weeping Angel attack in detail.

How do modern browsers work?

When you input data in your browser, you are essentially composing what is called a request packet. The browser then sends this request packet to the remote server, which analyses and computes a suitable answer. The remote server then sends back response packet(s) which is then displayed to you through the browser.

This request-response mechanism has been at the heart of internet browsing since the early days of the internet. Modern browsers not only provide an interface to stay connected with the world, but they also perform much more advanced tasks under the hood, while staying within the confines of this request-response mechanism.

Furthermore, reduced internet access costs and increased internet access speeds have resulted in modern browsers being increasingly used for various highly resource-intensive operations. These days, browsers have become an interface to access a multitude of powerful services such as serious (multiplayer) gaming, emulating entire operating systems, audio-video communication, to mention just a few!

Most websites are now mini-applications in themselves. Consider Google Docs, for example. There was a time when you needed to install a separate application (such as Microsoft Word) for your word-processing needs. Now, you can simply fire up your browser, visit the Google Docs website and create a new document --- just like that! What's more, all of the processing happens in the browser (and/or the remote server), and the document gets saved automatically to the cloud!

Sadly though, this change has not come without a cost. Modern browsers these days need to exchange a ton of data with the remote servers that host these websites, in order to present everything to you seamlessly. You already know that websites can (and do) ask your browser to share all kinds of data with them, ranging from the make and model of the browser to what devices are potentially present on your computer/device.

Since the browser always has full knowledge of both the request and response throughout a browsing session, it is highly critical that all data sent and received by the browser must be secured. Any leakage of data in this process has severe privacy implications and, therefore, every attempt

must be made to prevent this data from being accessed by unauthorized parties.

In the sections that follow, we'll be looking at some of the more popular browsers, some not-so-popular ones, understanding what browser plugins and add-ons/extensions do, and how you can effectively use them to keep your personal data safe on the internet.

[QRCode: https://wikileaks.org/ciav7p1/cms/page_12353643.html]

Moreover, almost all of these smart TVs have extremely overarching privacy agreements, in which you are (almost) forced to consent to wide-ranging data collection by the makers of the various apps and/or the TV itself. Scan the QR code given alongside this paragraph to read more about the various vulnerabilities in Smart TVs that have been exploited until now.

Popular browsers

The first graphical browser that was made available to the general public was called Erwise, and it was designed and developed as a student project at Helsinki University of Technology in 1992.

Today, however, the clear winner of the browser wars is Google Chrome -- a browser developed by Google that was quite a late entrant to the war. Google Chrome was first released in 2008 as a free browser for Windows users. It quickly gained popularity among the masses owing to its speed and clean, minimalistic interface – a popularity it still enjoys to this day, with a massive 70.71% of global market share on desktops and an equally massive 63.77% global market share across all devices, as reported by StatCounter.

[QRCode: https://hackaday.com/tag/smart-tv-hack/]

[QR Code: http://gs.statcounter.com/browser-market-share/desktop-mobile-tablet/worldwide/#monthly-200901-201907]

Statistically, eight out of every ten Indians reading this book are likely to be regular Google Chrome users and (judging by what we have learned about Google so far) all eight of them have been sharing their data freely with Google all this time. It is also likely that they have made no changes to the default installation on their devices and that all these eight Indians will continue to use Google Chrome because, they are already so used to it, you know?

Alexa, Siri, and Google

Maybe, it is due to the novelty of being able to talk to them or maybe it is the slight superiority one gets to feel while ordering them around but voice-activated tech has gotten increasingly popular with consumers over the last few years. Amazon's Alexa, Apple's Siri, and Google's Assistant have found themselves being increasingly tightly integrated with the various gadgets being sold by these tech companies.

What most buyers of these gadgets don't realize is that everything you that is said to Alexa, Siri, Cortana, or Google's Assistant is sent to the respective servers for processing purposes. The processing, in this case, involves converting the speech to text, parsing the text for commands, and sending back an appropriate response based on the command.

Furthermore, this processed audio doesn't get deleted immediately.

Sure, the tech companies claim that your audio gets encrypted in transit and is always stored securely in the cloud BUT did you know that the staff assigned to improving the speech-to-text accuracy for these devices is given access to a select subset of people's private recordings?

An April 2019 investigation by Bloomberg revealed that a specific mix of people hired by Amazon (which includes both employees and contractors) were assigned to listen to these audio recordings and annotate them for training the speech recognition software. In fact, on some occasions, some of the recorded audio was found to be inadvertent, that is, the voice-recognition software wrongly interpreted random sounds like the wake word and accidentally recorded entire private conversations that were then uploaded to the cloud, where they were then (in some cases) heard by these subcontractors.

In other words, some of the machine-learning and artificial intelligence displayed by these devices may possibly have had a human intervention and, as a result, some private details may have been heard by people that it was definitely not intended for.

Smart appliances

Do you think your refrigerator could snitch on you? Do you believe your thermostat could kill you? Or hold you to ransom? Or your doorbell? If I told you, your toaster might have participated in breaking the internet, would you believe me?

Well, each of those situations is entirely possible and, in fact, has happened.

In 2015, a team of hackers managed to exploit a smart refrigerator to reveal the Gmail credentials associated with the calendar that was being displayed on the screen of the fridge. The same people also managed to exploit a smart thermostat, gained control over it and displayed a 'ransom message' on its screen.

Later, in 2016, Russian hackers unleashed a botnet that exploited the weak security of IoT-enabled devices (such as your toasters, security cameras, baby monitors, and many more) in a worldwide DDoS (Distributed Denial of Service) attack that took down a bunch of sites on the internet, including The New York Times, Reddit, Twitter, Spotify, PlayStation, Paypal, and many others.

Privacy-aware browsers

If you are one of the eight Indians I referred to in the previous section and the thought of changing your browser makes you uncomfortable [1] , well, there's some good news for you.

Among some of the newer entrants trying to chip away at Google Chrome's market share are two browsers named Brave and Epic. Both of these are based on the Chromium open-source project (that is, they have the same look-n-feel) and use (almost) the same codebase as Google Chrome, except they don't send any data back to Google.

Brave browser

A relatively new entrant into the market, Brave browser has generated significant interest among privacy enthusiasts due to their strong stance on user privacy and their (intended) pay-to-surf model. Brave is completely open-source and they claim that their out-of-the-box installation settings are designed to be pro-privacy and anti-tracking, by default.

For instance, ad-blocking is made available by default in Brave. Or, the Safe Browsing option available in Chromium routes all safe-browsing requests to Google through a Brave-run server which doesn't keep any logs or store your IP. Brave also recently introduced private tabs with Tor for enhanced security and privacy while browsing.

Info

Brave's Pay-to-Surf Model

Yes, you read that right -- Brave intends to pay you to surf the web. The Brave Rewards program pays users in Basic Attention Tokens (BAT) for viewing ads from the Brave Ads program.

Brave claims that these ads are privacy-preserving and will be shown to Brave users in a non-intrusive and non-disruptive manner. Users will receive BATs (on a monthly basis) for viewing these ads. Brave Ads are opt-in by default and are matched directly to you on your local machine rather than a remote server, that is, your personal data never leaves your device. Brave claims that the only information they receive is accounting information to report campaign performance and delivery for advertisers.

However, there is no way to currently withdraw BATs and you can only spend them by donating them to your most visited websites or tipping content-creators who are Brave-verified, such as Wikipedia, and more. There are plans to allow users to withdraw their BATs into local currency or redeem them for real-world rewards but, as of August 2019, there is no clear date on when that is likely to happen.

[QRCode: https://en.wikipedia.org/wiki/2016*Dyn*cyberattack]

It is estimated that there are readily available botnets that can deploy more than three lakh IoT-enabled devices to unleash a DDoS attack at any given target.

However, that's not the scary part. The scary part is this:

Your IoT-enabled device may already be compromised. It might even get used as a part of a massive botnet in a future DDoS attack -- that means one (or all) of your IoT-enabled devices may be partly responsible for a future DDoS attack, and you won't even realize it!

[QR Code: https://brave.com/brave-rewards/]

RohitRecommends

I cannot deny that we are headed towards a future where all technology is connected, and all devices are capable of speaking to each other. At the same time, I feel it is important to keep track of what information is being shared between these devices. Choosing to ignore this puts us in a situation where we can be affected (or even harmed) by the information asymmetry thus generated.

The recommendations we have chosen to propose are, thus, based on the following guiding principles:

Knowledge of information-sharing, that is, being aware of what information by devices, is being shared and who has access to it, at all times.

Knowledge of interference, that is, having the ability to make changes to the quality and quantity of information being shared, at any time.

Execution of interference, that is, taking concrete steps to actually make changes to the quality and quantity of information being shared, whenever and wherever deemed necessary.

Using these guiding principles, we’re going to figure out a suitable system to deal with the privacy issues that may arise from the usage of smart devices.

BASIC: (1 point)

Regardless of what you think about smart devices and the IoT, it is extremely critical that you know and understand the length and breadth of data-sharing that these devices indulge in. That means, having full knowledge of what data is being shared and who (potentially) could have access to it.

Most devices require companion apps to be installed, and these companion apps may or may not collect additional data, on top of the data collected by smart devices. You need to be fully aware of all the data that is being collected in both cases – the companion app, and the device itself. You also need to understand and accept the implications of this data being sent over the internet to be stored in remote servers.

Once you are equipped with all of the knowledge outlined above, you must weigh it against the potential benefits being offered by the smart device and the enhancement in the quality of life that the device brings and ask yourself the questions:

"Can I (or, do I) use this smart device regularly?"

"Does this service offered by the smart device (and its companion app) merit sharing all of this data about me in exchange?" (Remember the butler?)

"If/When I stop using this device, is it likely to affect the quality of my life negatively?"

If the answer to any of these questions is No then you might want to proceed further. If not, then you may safely skip the rest of this section and proceed to the next chapter.

INTERMEDIATE: (2 points)

Equipped with the knowledge acquired in the previous (Basic) section, we invite you to evaluate your position a little more rigorously here. The questions you need to ask yourself at this stage are:

"Do I absolutely WANT to use (or to continue using) this device?"

"Am I okay withthe data that is being shared by the device and its companion app?"

If you answered No to any of the questions, then your answer is clear: You need to stop using the device right away. You need to switch it off, delete the companion app, delete any public accounts or identities you may have made in the process, delete the data stored on the smart device and the remote servers, and forget that the device (or the companion app) ever existed in the first place. You may then skip to the next chapter.

If you answered Yes to BOTH the questions, then you might want to read further, that is, the Advanced section.

Epic browser

Like the Brave browser, the Epic browser is based on Google's Chromium project, but it is classified as commercial and proprietary software, that is, their source code is not open to review. While this may be a conscious decision to implement privacy-thru-obscurity, it goes against the spirit of transparency which is essential to be considered privacy-aware.

Epic also comes with extreme privacy enabled by default, including settings such as comprehensive ad-blocking, no history, no pre-fetching, no auto-fill, anti-fingerprinting measures, and many more. Epic also boasts of a one-click encrypted proxy to hide your IP address and encrypt your browsing. Furthermore, their privacy policy (rather uniquely) is written in plain English and mentions that usage data is neither collected from Epic browser nor stored on any servers.

While all of these features make Epic a mouth-wateringly lucrative option, the unavailability of source code is a huge flag that cannot be ignored.

ADVANCED: (3 points)

We do NOT recommend doing this unless you exactly know what you are getting into. Please ensure that you have expert supervision/consultation when you attempt this!

It is possible to use the smart devices and their companion apps in a manner that insulates the data being sent by them from the rest of the traffic on your network. This, however, requires significant technical knowledge and expertise of computer networks and internet traffic monitoring. You can find detailed guides on the internet by searching for appropriate keywords, such as Isolating [SMART DEVICE NAME] on Home Network or something similar.

Here’s a broad explanation on how this is done:

Create a separate (hidden, maybe?) secondary network for your smart devices.

Ensure that this network is properly firewalled and that it does not leak into your primary network.

Use this network (and only this network) to connect smart devices to the internet.

Use a separate smartphone/tablet for the companion app, and use the secondary network to access the internet on this smartphone/tablet

If you’d like, you can install an additional VPN to create a secondary layer of separation between the network and the internet.

The Tor browser

The name Tor has been adopted from the acronym for The Onion Router -- a worldwide network of servers initially developed with the US Navy to help people browse anonymously.

Using the Tor browser is akin to playing a game of Chinese Whispers over the internet; that is, it makes your request hop across multiple servers before routing your requests to the desired destination. The remote server responds back through the same path, thereby ensuring that your privacy is maintained behind a thick veil of whisperers . Since all communication is encrypted, none of the servers in the path can read it and, more importantly, none of it can (theoretically) be traced back to you.

To ensure this level of anonymity, Tor relies on a few basic principles:

Hides your identity: Tor does not ask for, store, or share any user data with any remote server

Removes trackers: Once you close the Tor browser window, all browsing history and data is erased.

Encrypted communications: All communication between the Tor browser, all the nodes along the route, and the remote server are end-to-end encrypted.

Due to the philosophies inherent in its design, Tor is the closest a browser can come in terms of achieving anonymity and maintaining your privacy on the internet, and I strongly recommend the Tor Browser for everyone wishing to surf privately and anonymously on the internet. There are a few downsides to using Tor, though.

Tor relays have often been abused by automated programs (a.k.a. bots) to harass and bring down websites anonymously. As a result, many websites have installed abuse prevention mechanisms in the form of human verification challenges (that is, CAPTCHAs and verification questions) that are presented to users accessing such sites via the Tor Browser. Users may find their browsing experience is noticeably slower than normal since the traffic hops across three different relays. Websites that automatically serve content based on your location will serve you content depending on the geolocation of your exit relay.

It may seem overkill to bounce your traffic through multiple different relays in different countries; it may be absolutely warranted in certain situations. Tor was primarily built for anonymity over the web. It was built as a tool for people to avoid tracking, for journalists to communicate without government interference, for law enforcement officers to track unlawful activities, for activists to escape surveillance -- essentially, Tor was built to help individuals seeking privacy and anonymity on an increasingly un-anonymous and heavily personalized web.

EXPERT: (5 points)

I only have two specific recommendations here:

Stop, I repeat, STOP using smart devices and/or IoT.

Do not; I repeat, DO NOT use any smart devices or IoT-enabled devices.

Is Tor truly anonymous?

Short answer: Yes, and No.

Long answer: Any service that promises anonymity will always have adversaries looking to infiltrate it and the same applies to Tor, as well.

Tor primarily relies on a huge network of volunteers and organizations to run the Tor relays that constitute the Tor network. There is a very real possibility that one (or a few) of them could have already been compromised by adversarial actors -- either state or non-state.

In fact, in 2014, a coalition of government agencies managed to take control of many hidden Tor services and took down the notorious the deep-web drug marketplace, Silk Road 2.0, its proprietor, and 16 others in a high profile bust. In the aftermath of the news, a lot of people were left asking this very same question, Is Tor truly anonymous?

To their credit, the people behind the Tor project responded by posting a detailed blog post evaluating andanalyzing all the methods that could have been used to execute this high profile bust. You might want to read the whole thing over on their blog; it's titled, Thoughts and Concerns about Operation Onymous.

Conclusion

Smart devices and appliances definitely have their uses. They provide us with services that attempt to make our life easier. However, until their security is strengthened, they will continue to remain a liability rather than an asset.

There are products available in the market that will help you protect your IoT-enabled devices from intrusions. There are steps you can take yourself to mitigate such attacks and to ensure that your smart devices do not get captured into a botnet. There are ways to ensure greater security for all the devices in your network.

However, there is only one guiding principle that I will advise to everyone who wishes to use any smart devices: If there is some information you don't want to share with the world, make sure that any and all of your devices do NOT have any access to that information. That means either isolating that information from the rest of the world or isolating all your devices so that they do not have direct access to that information.

Regardless of which option you choose, you will have to ensure that this status quo does not change. Ever.

[QR Code: https://blog.torproject.org/thoughts-and-concerns-about-operation-onymous]

The gist of the story is this: Over the years, Tor has faced multiple attacks by adversaries -- both state and non-state actors -- trying to infiltrate its systems through various means. While utmost care is taken to protect the hidden services, no system is 100% perfect. The government agencies in question probably managed compromise or commandeer some Tor relays and/or exit nodes which, combined with OPSEC mistakes committed by the culprit, proved to be crucial in taking down the whole operation.

In other words, if a three-letter agency with (arguably) unlimited resources and singular interest in uncovering your secrets decides to take an interest, there's not much you can do, can you?]

Chapter 7

Desktops - Operating Systems

Privacy settings

Regardless of which browser you use, there are a few settings that can be tweaked to achieve a higher level of privacy and anonymity from websites attempting to profile you and your browsing habits. I strongly recommend that you spend some time working through this section -- especially if you haven't changed any settings on your browser since the day it was installed. If left unchecked, default installations of all popular browsers are designed to share a lot of data about you and your browsing habits, with their respective remote servers.

In the following sections, I provide you with a list of the most important browser settings that need to be changed to enhance your privacy while using your preferred browser.

Introduction

Regardless of how many smart devices we own, we still use desktop computers and/or laptops on a daily basis. In fact, quite a few of us use separate machines for home use and office use. It is extremely important to ensure that you maintain the highest level of security for both these machines since they are quite vulnerable to a range of adversarial attacks -- especially those that are connected to the internet, which is probably all of them.

Typically, the average user will use at least one of the following three kinds of PCs during their lifetime:

Home computer

Work computer

Unknown computer

Now, the first two categories are pretty much self-explanatory. The third category, (that is, Unknown computer) refers to all computers that do not fall under the first two categories. Thus, computers at a cyber-café, computers that you borrow from someone, computers you inherit – basically, any computer that has not been purchased and set up by you personally (or your office) will be classified as an unknown computer for purposes of this book.

Obviously, you cannot guarantee that your data will remain secure and private on any machine other than your own -- not even your work computer since your IT department gets to decide administrative policies for that computer. However, there are ways in which you can still ensure the security and privacy of your data on such computers, too. As with most devices, you have a wide range of options for securing such computers; you can secure them just enough or a lot, depending on how careful (maybe even, paranoid) you want to be about your data.

In the following sections, we'll take a look at the various machines you are likely to access and how to go about ensuring the security and privacy of your data on each one of them.

Private windows

One of the simplest changes you can make to your browsing habits is to use the privacy-aware browsing mode in your browser. This mode goes by different names for different browsers -- Chrome calls it Incognito , Firefox calls it Private , and Edge (as well as IE) calls it InPrivate . Whatever the name, the idea behind the concept remains the same -- this mode provides the user with a browsing session in which all of the information sent

and received within the session is completely erased at the end of the session.

Operating systems

The operating system is the primary agent that connects you to the rest of the internet. Programs on your system use the operating system to acquire your input, analyze your input, access the underlying hardware, perform various tasks based on your input, and present you with results.

It stands to reason, therefore, that having a privacy-aware operating system should be extremely important since the operating system can 'see' everything you do on your computer.

In case you are wondering, no, you can't turn this off.

Since the operating system needs to interact with various parts of the system, it must have access to them. If it has access to them, it can (and must be able to) examine all of these parts. If it can examine all of these parts, it can also keep a detailed account of everything that is happening with the system. There is no turning this off without interfering with the core working philosophy of the operating system. The best you can do is trust the operating system (and its developers) to not share this information with anyone else without your knowledge and consent. The notion of privacy and security when dealing with operating systems is, this, largely predicated on one factor – trust.

At the same time, you can (and must) take steps to ensure that you do not end up sharing this information with untrusted parties -- either by accident or on purpose -- which means, you will need to adopt a more secure, more privacy-aware approach with regards to your digital behaviors. In other words, to use the old cliché:

Trust no one, not even yourself.

In the sections that follow, we'll take a look at the various privacy and security issues that can arise while using various operating systems on a day-to-day basis. We'll look at enhancing user privacy by securing your accounts, by controlling the various (baked-in) telemetry options, and by carefully inspecting the applications installed on the system.

Telemetry opt-out

All three of the most popular browsers in use today -- Google Chrome, Mozilla Firefox, and Safari – have some kind of tracking or telemetry enabled out of the box. All of them claim that any and all telemetry data sent to them is anonymized and collected mainly to improve performance. I think you should be at least made aware that you have the option to opt-out of it.

Microsoft Windows

Since its release in 1985, Microsoft Windows has gone from strength to strength as the operating system of choice for the average PC user. In spite of facing tough competition from rival Apple from time to time, Windows has blown the competition away thanks to its user-friendly interfaces and adaptability to most modern hardware. While Apple insists on providing fully integrated machines, i.e. machines designed for immediate personal use, Windows is often preferred by people because it allows for a wide range of customizations -- something Apple doesn't provide with equal ease.

Thanks to the licensing model adopted by Microsoft, the Windows operating system can be installed on a variety of devices built by several PC manufacturers such as Dell, HP, Toshiba - to name just a few. Savvy enthusiasts can build their rigs as per their requirements, mixing and matching various components to suit their specific needs. Gamers can build PCs using configurations with powerful graphics cards, while people-on-the-go can choose PCs (laptops) with longer battery life, and home users can choose something less expensive to fit their budget. Windows has been proven to run on most, if not all, of these configurations without a hitch, which makes Windows the OS of choice for most people.

As of January 2019, according to Statista.com, Windows had around 75% of the market share when it came to operating systems on personal computers. It is also worth noting that Windows has remained a dominant presence in the personal computer operating system market and that their market share has never dipped below 70% since 2013. In India, according to Statcounter.com, Windows dominates the market with around 80% of the market share, as of June 2019. 46% of Indian Windows users run Windows 10, 43% run Windows 7, and all the other versions of Windows make up the rest.

Clearly, Windows 7 and Windows 10 are the OSes of choice for Indians. Therefore, in this chapter (and the chapters that follow) I've chosen to focus a majority of my discussion and evaluation around these two choices.

However, its popularity also makes Windows the primary target OS for hackers and other malicious actors, which is why most malicious software affects Windows more than it does the other two OSes, viz. macOS, and Linux.

Note

It's not true that they (macOS or Linux) don't have viruses; it's just that there is little interest in spending significant resources in developing viruses, malware, and other attack vectors for an OS that has barely 14% of the worldwide market share. If anything, the argument that

macOS/Linux doesn't have viruses applies only due to the disinterest of the attackers rather than actual vulnerability issues.

In any case, the fact that Windows has such a large attack surface means that we need to be extremely careful about ensuring that our data is private and secure when using this OS.

Syncing and personalization

All popular browsers provide the option of syncing your activities on the browser with the cloud. If you are logged in, your browser will offer you the option of storing one or more of the following -- your bookmarks, your history, your open tabs, your logins, your extensions, and settings -- from your browser, in the cloud. The advantage of syncing all this data is that it helps you maintain a uniform browser interface by syncing with the cloud. However, it also means you are sharing all of that data with a third-party that may or may not be able to keep this data absolutely private.

While it is extremely tempting to keep everything synced to the cloud, I recommend that you only sync the extensions and settings, if you absolutely must. I strongly recommend AGAINST logging in and/or syncing your data, for obvious reasons or privacy and anonymity.

Modern Windows (Win10, Win 8.1, and Win8)

Three years after the release of Windows 7 in 2009, Windows 8 was made available to the general public in October 2012, with Windows 8.1 following a year later in October 2013.

Both of these operating systems were received rather critically by the users, because of the sudden shift in the design, as compared to Windows 7. Many users across the internet reported the absence of the traditional Start menu and taskbar as being one of the major drawbacks of the new version of the operating system. Noting all of these concerns, Microsoft launched Windows 10 in July 2015 and gave licensed users a full year to update straight from Windows 7 to Windows 10 for free.

The strategy seems to have worked since Windows 10 is now reported to have a 58% usage share of all Windows versions on traditional PCs (with Windows 8 and 8.1 accounting for a combined 7.5%) as of July 2019. (Source: StatCounter Global Stats, Desktop Windows Version Market Share Worldwide).

Search engine integration

So powerful is Google's presence and reputation as the best search engine on the internet that all the popular browsers use it (that is, Google) as their default search engine. Although this reputation is well-earned, due to the quality of search results it offers, you must also remember that Google collects massive amounts of data every time you use their search engine. Therefore, I recommend using a more privacy-aware alternative [2] , such as DuckDuckGo or Qwant .

Furthermore, when you type in the address bar of the browser, you'll notice that your browser offers instant suggestions that appear as you type. This is because your browser sends everything you type, as you type to a search engine and retrieves those suggestions.

Cookies, tracking, and content blocking

Every website you visit stores a small text file on your computer called a cookie . This text file contains information about you, your system, and some data about your visits to the website. Some websites may also store third-party cookies (i.e. cookies from other websites, usually advertisers and/or social networks) on your system. Advertising networks use these cookies to track the user on multiple websites and gather their browsing information.

Cookies are the reason why you don't have to re-login when you accidentally close the browser tab or window. Cookies are also the reason why a specific ad keeps popping up no matter which webpage you open. Thankfully, all modern browsers provide an easy way to block third-party cookies.

[QR Code: http://gs.statcounter.com/windows-version-market-share/desktop/worldwide/]

Windows 10 operates on the OS-as-a-service model, meaning that features and updates cannot be selectively installed but instead are delivered and installed without any user intervention. In simple words, if you have Windows 8 or below, I would recommend that you upgrade to the latest version of Windows 10, as soon as possible.

Windows 7 and older versions

Windows 7 was initially supposed to be an incremental upgrade to Windows Vista, with tweaks made to improve hardware and software compatibility. However, continued criticism of Windows Vista resulted in Microsoft deciding to provide Windows 7 as a standalone version of the popular OS.

The decision worked in Microsoft's favor, with 100 million copies being shipped worldwide in just six months, increasing to over 630 million licenses by July 2012. As of July 2019, an estimated 32% of computers running Windows still run on Windows 7.

However, mainstream support for Windows 7 ended on January 2015, and extended support for Windows 7 ended on January 14th 2020. Users of Professional and Enterprise versions of Windows can opt to purchase Extended Security Updates that will offer additional updates for three years after extended support ends, that is, until 2023.

Forms and autofill

Over the years, forms have become an integral part of web browsing - in fact; we use forms without even realizing that we are using them! For example, when you login to a website, you are actually submitting a login form to the remote server, which then validates it and responds accordingly. Or, for example, when you buy something from a shopping site, you fill out a form with payment details, shipping address, and other relevant information. Most modern browsers have a form autofill feature that allows you to save time and fill out various forms at the click of a button.

Permissions andsite settings

The internet is accessed by a wide variety of devices with a wide variety of hardware. Most modern browsers are increasingly equipping themselves with various interfaces that can take full advantage of the various capabilities of your device. Thismeans browsers can now request to access location information.

Note

Remember all that data acquired from your phone in the first chapter? Well, a huge part of it was thanks to the fact that your phone browser runs JavaScript. With JavaScript and the modern browser, developers can make the browser do a lot of powerful things – both useful AND nefarious.

Therefore, under ideal circumstances, I'd recommend that you toggle JavaScript to Blocked as well. However, the vast majority of websites on the internet rely on JavaScript to provide many of their features and blocking them from using JavaScript often breaks their functionality. Toggling this setting to Blocked would significantly alter your browsing experience, so I'm going to recommend that you leave it as it is.

macOS

Over the last few years, Apple has consistently held a market share of about 9-10% in the Desktop OS market segment, i.e. one out of every ten desktops is running the macOS operating system. However, in spite of having such a huge lead over Apple, Microsoft's overall market capitalization was still reported to be less than that of Apple. In other words, Apple earned more out of its meagre 10% market share than Windows did with nearly 75% market share.

Sure, it can be argued that Apple sells its products at a premium, a much higher cost than Microsoft does, and that certainly explains its massive market capital. However, it can also be argued that they have consistently delivered products that are worthy of the premium pricing model they employ -- both in terms of usability and stability. Moreover, Apple consistently claims their products are designed keeping the user's privacy in mind and, to some extent; they have consistently delivered on this promise as well.

Furthermore, the fragmentation present in Windows versions is very rarely seen in Apple devices. As of October 2019, approximately 83% of all devices running macOS run version 10.13, 10.14, or 10.15 - the three latest updates. In comparison, only 50% of Windows machines run Windows 10, while 40% still run Windows 7 [1] .

Hardcore Mac enthusiasts claim that MacOS offers the perfect middle ground between Windows and Linux, that is, it is as easy to setup and use as Windows while being as developer-friendly as Linux due to its Unix-based origins. However, even though it is based on FreeBSD [2] , macOS is proprietary software.

You might also hear arguments from people, claiming that Macs are better than Windows because they don't get viruses [3] or that Windows is better than Macs because you don't need to use proprietary hardware all the time . The internet is filled with tons of arguments of why one is better than the other, but I'm going to bow out of that conversation here respectfully.

All I am going to say about the Mac vs Windows debate is that neither of them is truly secure nor do they truly respect the privacy of the user -- well, at least as much as most of the Linux-based operating systems do, anyway.

Info

Apple's Stance on User Privacy

As an operating system, Apple is a lot more considerate about user privacy as compared to Microsoft and Windows – at least, by their own description. On their privacy policy page, Apple claims that they can create personalized experiences without using personal information.

Plugins and extensions

Imagine, for a moment that you have just purchased a house. It is big, roomy, empty and it doesn'thave a garage. If you decide to build a garage, then you have extended the house. If you decide to add a utility such as air-conditioning or central heating, you have plugged in an additional component to your house. The extended garage can also utilize the air-conditioning' plugin.

While browsers are powerful applications in their own right, their utility can be further enhanced by the use of plugins and extensions.

Info

Extensions? Add-Ons? What's the difference?

Short answer: For this book, there's (essentially) no difference.

Long answer: Google Chrome and Safari both call them extensions, whereas Firefox, Internet Explorer and Edge refer to them as add-ons, but they all imply the same thing. Firefox uses the umbrella-term Add-ons under which extensions, themes, language packs, etc. are further separately classified.

I have used the term extension through this book to avoid any confusion, but I'd like to clarify that I mean the same thing whether I say extension or add-on .

In other words, they claim that the data they collect is mostly processed on your device itself. Apple may still send some usage data to their servers in some cases, the details of which can be found in their Privacy Policy. The data that does get sent back to Apple servers are scrubbed, anonymized with rotating identifiers, and only sent to Apple servers after you give explicit permission to do so.

[QR Code: https://www.apple.com/privacy/approach-to-privacy/]

The thing is, different apps and features on your macOS device will have different ways of treating your data. Scanning the QR code given alongside (in this section) will take you to a page on the Apple website titled Our Approach to Privacy where Apple has described -- in a lot of detail -- the various ways in which they try and safeguard the privacy of the data contributed by Apple users.

The difference

Linux

This may sound strange to you, but Linux isn't an OS by itself. The term Linux is often used to refer to a family of open-source operating systems based on the Linux kernel.

The first version of Linux was developed by a 21-yr old Finnish Computer Science student named Linus Torvalds as a personal project to create a free operating system to use on his new PC with an 80386 processor. From there, the Linux project grew, and eventually collected a dedicated community of various kinds of Linux enthusiasts.

You'll often hear the words distribution or flavor in conjunction with the Linux family of operating systems. A distribution (or flavour) of Linux refers to an operating system made by combining the Linux kernel with additional utilities (for example, GNU tools, X Window System, Desktop Environment) and assorted software (for example, package managers and other software) in a manner such as to meet the needs of the user.

Info

GNU's Not Linux!!

Notice that I used the phrase, 'a Linux-based operating system' This is because, contrary to popular opinion, Linux is technically not an operating system. It is the 'kernel' of the operating system.

In simpler terms, if I could draw an analogy to a restaurant, the kernel would (probably) be the restaurant manager who delegates work to the kitchen staff. The kitchen would be the system hardware, the various staff would be the 'drivers', and the entire restaurant setup would (probably) qualify as the shell .

More than six hundred such Linux distributions (or distros , as they are popularly called) exist today, and at least five hundred of them are under active development. These Linux distros can be either commercially-backed (for example, Fedora, openSUSE, Ubuntu, and many more) or entirely community-driven (for example, Debian, Gentoo, Arch Linux, and many more) and can be installed on a wide variety of devices such as servers, desktops, laptops, phones, tablets, and more.

One of the biggest advantages of having so many distributions is that you can choose a distribution that best fits your needs. Looking for something similar to macOS? There's ElementaryOS. Looking for something simple? Try Ubuntu. Are you looking for something lightweight? Maybe Lubuntu, Xubuntu, or Puppy Linux is more up your alley. Are you looking for something secure-ish? Well, you can try Qubes, TAILS, or similar distribution. There's a flavour of Linux for everyone.

That said, one of the biggest arguments against Linux is the unavailability of various tools and software that we take for granted on Windows, the biggest example of them being Microsoft Office. Instead, most Linux users rely on alternatives such as Libre Office, WPS Office, or web-based alternatives such as Google, and Microsoft Office Online to work with Office documents on Linux.

Note

As of July 2019, no official Microsoft Office installation is available for Linux, although you can still use the (somewhat limited) Office 365 version on your Linux machines. There are workarounds that allow you to run Microsoft Office on Linux machines, but none of them is officially recommended by either Microsoft or The Linux Foundation.

Lastly, while the newer versions of Linux are quite user-friendly, I must warn you that it has a different operating philosophy as compared to the other operating systems in the market. As a result, people switching to Linux often feel overwhelmed and may feel the need to immediately switch back to whatever OS they feel comfortable with.

However, in my opinion, once you get past the steep learning curve, you will soon realize that Linux is one of the most powerful, most secure, and most customizable operating systems you will ever use. This further evidenced by the fact that Linux is a major player in almost everything except the Desktop OS market. For example, the biggest companies use Linux-based servers, the fastest supercomputers run on Linux, and one of the most popular mobile operating systems, Android, is basically a port of Linux.

Plugins and extensions are fundamentally different

A plugin is an additional piece of software (usually third-party) installed alongside the browser that provides specific functionality excluded in the default browser installation. For example, when you watch Netflix videos in your browser, your browser usually invokes the Widevine Content Decryption Module -- a plugin that enables playback of encrypted media within the browser. Or, when you used to play flash games in your browser, you were actually invoking the Adobe Flash Plugin to perform this task.

An extension, on the other hand, is a (sort of) middleware that enhances the browser capabilities either through customization or manipulation of data received and processed by the browser. When you activate an adblocker extension, it processes the data received by your browser and performs its function, that is blocking ads.

In other words, an extension may sometimes invoke a plugin in the process of carrying out its tasks, but a plugin is always a standalone object that provides very specific functionality.

Multi-OS systems

All of the common configurations that we have seen so far have all involved computers with a single operating system, that is, the computers were configured to run one of the three available OSes, viz. Windows, or macOS, or Linux. However, it is possible to run multiple operating systems on the same computer without having one clash or corrupt the other. These configurations are commonly referred to as multi-OS systems and are only used in rare-but-specific scenarios.

We'll first take a look at the various multi-OS configurations and then evaluate potential scenarios for using multi-OS setups.

Potential security concerns with plugins

For a long time, browsers would depend on various plugins to execute some fairly processing-intensive tasks, such as loading embedded games, applets, or videos inside the browser window. It was fairly common to have browser invoke the flash plugin to play games and videos or invoke the Java plugin to display an applet. Being able to experience multimedia in your browser usually meant running one of these plugins in the browser window.

However, this capability came at significant risk -- these plugins often had security vulnerabilities that could be (and often, are) exploited by attackers to gain control over your system. Furthermore, since these plugins were maintained, updated, and released independently, updating them was often a separate process. Thus, anyone who chose/forgot/refused to update the plugin was instantly vulnerable to attacks that exploited the plugin's vulnerability.

Info

Flash was one of the biggest culprits in this regard with nearly 900 severe (that is, CVSS score >= 9) exploits discovered and published between April 2008 and May 2019, as per the listing available on www.cvedetails.com

In fact, in 2010, the frequent discoveries of Flash vulnerabilities even prompted Steve Jobs to declare that Apple would stop allowing Flash on iPhones, and he wrote a blog post titled Thoughts on Flash on the official Apple blog (QR code given alongside this paragraph) in 2010.

Dual boot

The most common multi-OS scenario is what is commonly known as dual-booting. It involves partitioning the computer hard-drive into two or more partitions and installing different operating systems on each partition. A special software tool called the unified bootloader is assigned the task of reading the various partitions and listing the various operating systems available on each partition.

In dual-booted (or triple-booted, or multiple-booted) systems, the user *must* choose the OS to boot into. Each operating system operates independent of the other, and all hardware resources are available for the operating system that is chosen at boot. To boot into another OS, the active OS needs to be shut down, and the machine needs to be restarted.

Typically, the 'dual-booting' setup is most commonly employed by users who are comfortable at working with multiple operating systems. Machines with Windows/Linux or MacOS/Windows (a.k.a. Hackintosh?) are the most commonly found dual-boot options.

[QR Code: https://www.apple.com/hotnews/thoughts-on-flash/]

In July 2017, Adobe finally announced that it would end support for the Adobe Flash plugin by 2020 and encourage the use of open HTML5 standards instead, as seen in this official blog post titled Flash & The Future of Interactive Content on the Adobe Blog. Scan the QR code given alongside this paragraph to read the entire blog post on your device.

Virtual machines

A virtual machine (popularly called a VM) is an emulation of a computer system running on another computer system, that is, a VM is a computer - called a guest - running inside another computer - called the host . Both computers share the same hardware resources, that is, the same processor, the same graphics card, the same storage, the same memory, and many more.]

The advantage of using VMs is the availability of multiple configurations on one single machine, that is, you can have multiple guests running many different distributions of Linux, all on the same host – though, not necessarily at the same time. However, since VM access the hardware indirectly through the host, they can often be inefficient and sometimes hinder the performance of the host system.

That said, for users looking to try out Linux, I highly recommend installing the latest version of a popular Linux distro (for example, Ubuntu, Mint, or Elementary OS) in a VM on an operating system you are already familiar with, such as Windows or macOS. The internet is full of multiple step-by-step guides, videos, and tutorials that will help you do this on your PC or laptop.

[QR Code: https://theblog.adobe.com/adobe-flash-update/]

Modern browsers have already begun the process of replacing these plugins by adopting open standards and encouraging alternative languages and technologies. The uniform adoption of open standards has allowed web developers to create amazing, fun, and useful applications without having to rely on proprietary code, such as Adobe Flash, Shockwave, Java, and many more.

Live OS

A Live OS is an entire, functional operating system that can be booted off a detachable storage volume, that is, a USB, a DVD-ROM, or a CD-ROM. While the latter two options (viz. a DVD-ROM and a CD-ROM) are not used as frequently in this day and age, I have mentioned them here as they constituted the first iteration in this concept. Many operating systems including macOS, Windows, and multiple Linux distros can be made available as Live USB.

Lightweight operating systems, installed on bootable media (such as CD and DVD-ROM drives) and equipped with command-line interfaces, were initially used by technicians and computer enthusiasts to repair booting issues on computers. These soon gave way to Live USBs with the introduction of USB booting in personal computers in the early 2000s. These live USBs were superior to their CD and DVD counterparts due to the ability to read AND write the data stored with the OS. Moreover, since moving parts are absent in USBs, it allowed for faster read times, thus ensuring that a live OS on a USB could be booted fairly quickly as compared to a Live CD.

These days, most live operating systems allow for full read and write access, meaning you can make persistent changes to the operating system. These changes can be made to the bootable USB itself or can be written to the persistent storage on the computer's hard-drive. As a result, most live operating systems available today can be classified into two major types -- persistent and ephemeral.

Potential security concerns with extensions

While plugins are bits of (usually proprietary) third-party code running within the browser, extensions are bits of code that usually perform certain tasks on the web page before it is displayed (or while it is being displayed) to the user. For example, uBlock Origin is an adblocking extension which scans webpages received by your browser and removes ads from the page. That said, everything that I have said in the previous paragraphs about plugins is also somewhat applicable to extensions.

If you are thinking, If an extension can access all webpages, then it means the extension has access to everything I view while it is installed, which means my browsing history is not private at all!, you would be absolutely right. Malicious extensions can disguise themselves and quietly siphon away your data in the background -- a recent leak of private FB messages from 81000 accounts was carried out in this manner.

Tips

While installing extensions…

There are a wide variety of extensions and add-ons available for your browser, and it is important that you choose carefully the extension you want to install. To that end, I have compiled a few simple rules of thumb you must follow while installing extensions for your browser:

Trust and verify: Always install extensions only from trusted, vetted, and verified developers and sources. Google has a vetting policy (called Project Strobe) for extensions on the Chrome Web Store to ensure that all extensions on the Chrome Web Store are trustworthy by default. Mozilla uses the Recommended Extension badge to indicate that the extension has undergone a security review.

Everything in moderation: Only install the extensions that you absolutely need and use. The more the number of extensions on your system, the greater are the chances of one of them going bad or rogue and infecting your system.

Prefer open-source extensions: Even if you can't read code, people who can, will usually quickly shut down (or fork away from) extensions that have malicious code, thus inoculating you from any potential harmful effects.

Eternal Vigilance: Keep your extensions up-to-date and ensure that its code continues to remain uncompromised. Good extensions can very quickly turn bad, for example, in 2017, the Web Developer extension for Chrome was hijacked, and a malicious update was pushed out to users which caused ads to appear during browsing sessions.

Data persistence

Some live USBs allow you to make changes to the live operating system, and these changes are persisted across reboots. For instance, while running the Live OS, if you were to install specific software or download a specific document or file to the system, that software, or document, or file can be made available each time the system reboots.

Data persistence can be limited or full-install, that is, you can choose only to persist data across sessions (either on the USB or local storage) or you can choose to install the full operating system on the USB. Although installing the entire OS on the USB ensures greater security and faster boot times, it must be noted that not all operating systems allow for full installations on the USB. Moreover, installing the entire OS on a USB requires a significant amount of storage space to ensure that both the OS and user data can be accommodated.

For most use-cases, using a Live OS with data persistence across sessions is a great way to test-drive various Linux distros before fully installing them on your computer. However, this data is usually left unencrypted, so there is some amount of risk involved if you happen to lose the physical USB drive.

Leave No Trace

In contrast, you can choose to NOT persist any data across reboots. Each reboot of such a live OS results in a version of the operating system identical to the one that was booted during first-run. These operating systems run solely in the available RAM and do not write anything to the host storage system. As a result, they leave no trace of their existence and are also called amnesiac operating systems.

Such amnesiac live operating systems come in very handy whenever you use any machine/s in a semi-private or public setting/s that you do not trust, for example, your neighbor's computer, or computers at cyber cafes, exhibitions, public libraries, and many more. Since the Live OS operates only within the confines of the memory, no data is written to the host system's hard disk, that is, it leaves no trace on the host system.

I therefore strongly recommend that you always carry a bootable USB with an amnesiac Live OS (such as Tails, Subgraph, or Qubes OS) in case you have to use an unknown computer in a semi-private or public setting. This will ensure that you do not accidentally share any data on unknown machines and will provide you with a familiar and secure OS environment to work with.

RohitRecommends

By all accounts, Google Chrome is the browser of choice for most people surfing the internet, leaving all other browsers far behind. Indians, too, overwhelmingly choose Google Chrome as their browser of choice, with 81.15% market share on the desktop and 66.4% market share across all devices.

While there are ways to make Google Chrome more privacy-aware, I would recommend avoiding it instead. Due to the business model they have implemented, the entire Google ecosystem is designed to give you as little privacy as possible. Therefore, in my opinion, the less you use Google products, the better it becomes to maintain the privacy of your data.

Therefore, most of the recommendations in this section will be made under the assumption that you are NOT using Google Chrome. Wherever possible, I will try to include relevant options for Chrome, but I do NOT endorse it. Furthermore, some of my recommendations for Mozilla Firefox will also apply to Google Chrome, although the wording involved may be different from what you'll read in this book.

Important!!

In the sections that follow, there will be a lot of recommendations which will feel extremely overwhelming at first glance. You might even think, That's a lot of work for just a few points! and, technically, you would be absolutely right.

Which is why, I propose a 5x multiplier for each recommendation level, valid ONLY for this chapter.

How does that sound? Good? Okay then, open your browser and start earning your points!

Default user: administrator vs guest

One of the biggest security mistakes (usually on Windows systems) that most users make is using their operating systems under the default administrator account, and often without a secure password. This is highly risky since anyone with physical access to the system can log in and install malicious software (such as keyloggers, Trojans, and many more) without the owner's knowledge or permission.

Typically, most operating systems recognize three classes of users:

Administrators: These are accounts with elevated privileges, that is, controls all the critical administrative functions such as installing and removing programs, adding and removing users, device maintenance, adding and removing restrictions, and many more. Basically, these accounts have the privilege to do anything and everything that has the potential to affect system performance. These are called administrator accounts in Windows, and root on macOS and Linux systems.

Standard users: These are standard accounts that can access most functions of the computer (such as running various programs), but they aren't allowed to make any significant changes (installing programs, adding/removing users, and such) to the system. Windows refers to these as standard accounts, while macOS and Linux refer to them as simply user accounts.

Guest: A Guest account is (usually) a password-less account, available only on Windows and macOS systems. Any user can log in to the computer as a Guest and access various programs on the system. In Windows systems, any downloads, documents, files, etc. created or saved under a Guest account will persist across sessions, whereas on Apple systems, everything created during a Guest session is deleted after the user logs out.

Only Linux insists on creating standard accounts for users during OS installation. For both Windows and Apple systems, it appears as a recommended step, but it is not mandatory to create a non-administrative user during installations. The primary user of both macOS and Windows systems is, by default, an administrator account by default. Therefore, I strongly recommend that you create a separate, standard user for daily

use -- either during installation or when you log in for the first time.

Both macOS [4] and Linux allow for further control over user accounts through the use of user groups. You can define various user groups and give each user group specific access to your system. For instance, you can define a group that only has access to certain devices, for example, a printer, to ensure that the printer is not overused.

BASIC (5 points)

Telemetry

Telemetry refers to the automated collection and remote monitoring of data and measurements from a device, or devices. The data collected through telemetry is typically used to understand various kinds of patterns created in the process of using the device. Typically, for operating systems, telemetry may be used to understand how various features get used, or diagnose errors arising out of device usage, or measure performance and other related metrics.

A lot of times, when I (or other privacy and security experts) say that your devices are sharing data without your consent, I (or we) are usually referring to telemetry. My issue with telemetry is that the data collected through even the most basic telemetry exercise can be easily leveraged and manipulated to create profiles of individual users, which is rather detrimental to user privacy [5] .

Let's look at the telemetry behaviors of various operating systems, shall we?

Browser recommendation

I recommend using any of Mozilla Firefox, Safari, or Brave [3] since all three of them (seemingly)provide several additional ways for users to tweak their privacy settings.

Both Firefox (and Safari) have a good track record in terms of user-privacy and data-security, until now. Firefox is developed and maintained by Mozilla -- a non-profit organization -- who claim that their mission is to keep the internet open and accessible to all. Safari, on the other hand, is the default browser that comes bundled on all Apple devices, and it follows Apple's privacy and security philosophy in its design.

A recent analysis of popular web browsers posted in July 2019 on the ExpressVPN blog ranked both Safari and Firefox higher than Google Chrome. Scan the QR code displayed alongside to read the article titled Ranked: Security and privacy for the most popular web browsers in 2019 on the ExpressVPN Blog.

Windows 10 telemetry

One of the biggest arguments against Windows 10 that you'll hear from various privacy advocates is the automatic data collection spread across various features of Windows 10. Many privacy experts have even gone so far as to call it a privacy nightmare because of the amount of data it collects from its users.

Right from the moment it boots up for the first time, Windows 10 constantly sends back data collected through various user interactions to Microsoft servers. Every time you search for something on your PC, or connect to a Wi-Fi network, or update your OS, you voluntarily share your data with Microsoft servers, which is then used to improve your Windows experience .

[QR Code: https://www.expressvpn.com/blog/best-browsers-for-privacy/]

I'll be outlining these tweaks shortly, so make sure that you apply those tweaks if you want to optimize, the privacy of your personal data.

Info

Why not Tor, instead of Firefox, Brave, or Safari?

Ideally, using the Tor browser would ensure maximum anonymity and, therefore, maximum privacy. However, remember that Tor has the unfortunate effect of slowing down your browsing speeds -- not recommended if there are important tasks to be done in a hurry. Furthermore, logging in to an online account (any account) while using the Tor browser actually compromises your privacy, if you've logged into the same account from other browsers.

Essentially, what I'm saying is, if you're using the Tor browser, use it independently from other browsers, that is, that is, stuff that you do in the

other browsers and stuff that you do in the Tor browser should be kept separate and exclusive.

Diagnostics and feedback

No matter how much you restrict them, Microsoft still collects what they call basic diagnostic data, which they define as follows:

Basic diagnostic data is information about your device, its settings and capabilities, and whether it is performing properly. This is the minimum level of diagnostic data needed to help keep your device reliable, secure, and operating normally.

You can see this for yourself in the Windows 10 Settings application. Click on the Start menu, then click on the Settings gear icon, and click on Privacy . Then, click on the Diagnostics & Feedback section in the sidebar on the left.

Private browsing

Regardless of whether you are using Google Chrome, Mozilla Firefox, Safari, Brave, or any other variant, I recommend using the privacy-aware browsing mode for any and all kinds of casual internet browsing.

This is because no data (such as history, cookies, and many more) is stored in such private browsing sessions. So, if you use a shared computer at home, work, or anywhere, I recommend that you always use the privacy-aware mode.

However, do remember that the privacy-aware browsing mode does not make you truly anonymous in any way. It merely prevents other users of the same system from being able to see any activities conducted during this browsing session. Your network administrator, your ISP, any websites you visit, and any people physically next to you will still be able to see and track what you do during this privacy-aware browsing session.

To open a privacy-aware browsing window:

In Firefox: Use the New Private Window option in the hamburger menu on the top right or press Ctrl+Shift+P in an existing Firefox window. A new window will open informing you that You're in a Private Window .

In Safari: Use the New Private Window option in the File menu on the top right. A new window will open informing you that You're in a Private Window .

In Chrome: Use the New incognito window option in the three vertical dots menu on the top right or press Ctrl+Shift+N in an existing Chrome window. A new window will open informing you that You've gone incognito .

Note

Safari does not have a keyboard shortcut to open a private window but you can assign one manually by going to System Preferences | Keyboard & Mouse and clicking on the Keyboard Shortcuts tab.

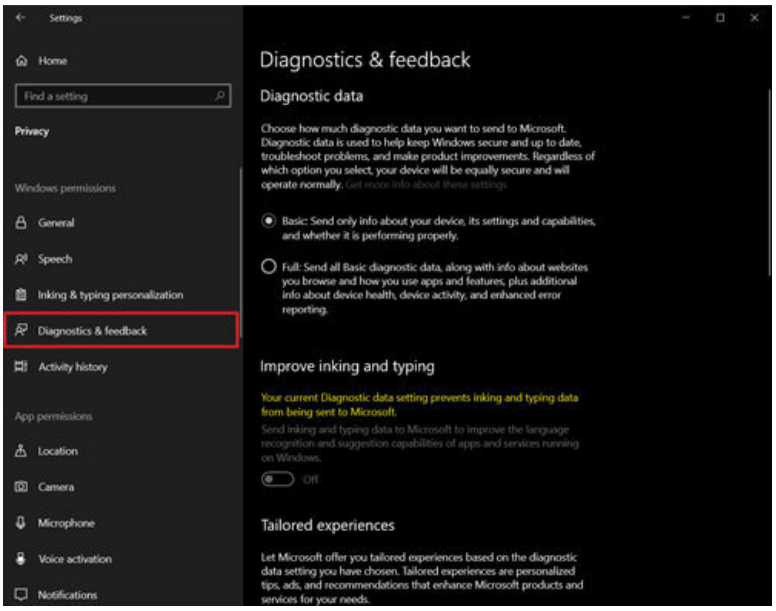


Figure 7.1: Screenshot of the Diagnostics & Feedback section under Settings > Privacy in Windows 10 (v1903)

What's even more worrying is the description under the second option, named Full because this is theoption that is enabled by default. Under full diagnostic data , Microsoft collects a comprehensive amount of data about your system and your actions on the system, which it describes as

follows:

Full diagnostic data includes all data collected with Basic, along with information about the websites you browse, how you use apps and features, plus additional information about device health, device activity (sometimes referred to as usage), and enhanced error reporting. At Full, Microsoft also collectsthe memory state of your device when a system or app crash occurs (which may unintentionally include parts of a file you were using when a problem occurred). While your device will be just as secure and operate normally, if you choose the Basic level of diagnostics, the additional information we collect at Full makes it easier for us to identify and fix issues and make product improvements that benefit all Windows customers.

If you want to see what data is being collected exactly, scroll down, toggle the section titled View diagnostic data on, and click on the button underneath named Open Diagnostic Data Viewer to download the eponymous tool from the Microsoft Store. Install the tool and wait for a few days for it to collect the data.

Privacy settings

Once you have chosen your preferred browser, we'll need to ensure that your browser settings are optimized for the best data-privacy possible while ensuring that your browsing habits remain unaffected. In order to achieve this, I'll be recommending a few changes that you will want to make in the Settings [4] (or Options , or Preferences) of your browser to ensure the privacy of your data.

Important!!

The recommendations that follow are specific to Mozilla Firefox, but the overall philosophy is applicable to some of the other browsers as well. I'll try and cover a couple of other browsers, but I strongly recommend switching to Mozilla Firefox.

Mozilla Firefox

First, ensure that your Firefox installation is absolutely up-to-date by going to Menu | Help | About Firefox. A small window will pop-up telling you whether Firefox needs to be updated. If it does, download and install the update and then restart the browser for the changes to take effect.

Once you have updated your Firefox browser to the latest version, go to Menu | Options or type about:preferences in the address bar of your Firefox window and press Enter . Then, one-by-one, follow all of the recommendations listed below:

Opt-out of telemetry and collection of usage data: Click Privacy & Security in the sidebar, scroll down to the section titled Firefox Data Collection and Use and uncheck the checkboxes titled:

Allow Firefox to send technical and interaction data to Mozilla.

Allow Firefox to send backlogged crash reports on your behalf.

Turn off syncing and personalization: Click Sync in the sidebar and check if you are logged in to your Mozilla account. While it is extremely tempting to keep everything synced to the cloud, I recommend that you only sync the extensions and settings, if you absolutely must.

Change your default search engines: Click Search in the sidebar and in the dropdown available under Default Search Engine, switch to a more privacy-aware alternative such as DuckDuckGo instead of Google. Click the link titled Find more search engines under the One-Click Search Engines section to search for and add additional search engines.

Search suggestions: Disable the search-as-you-type (or search suggestions) feature by unchecking the checkbox next to Provide search suggestions .

Cookies, tracking, and content blocking: Click Privacy & Security in the sidebar and under Enhanced Tracking Protection , choose Strict for better protection of your browsing data. I also recommend Always choosing under the Do Not Track setting.

Permissions and site-settings: Click Privacy & Security in the sidebar, and, under the section titled Permissions :

1) One-by-one, click on each of the Settings buttons next to Location, Camera, Microphone , and Notifications and select the checkbox titled Block new requests to access [XYZ] , where [XYZ] refers to the feature whose settings are being looked at.

2) Click on the Settings button next to Autoplay and change the Default for all websites to Block Audio and Video in the dropdown.

3) Next, select the checkboxes next to Block pop-up windows and Warn you when websites try to install add-ons .

Once you've completed the recommended actions above, go through the list again and see if there is anything you (or I) may have missed. Mozilla may have added new privacy features to Firefox between the time this book was written and by the time you are reading this. If you find something not covered in this set of recommended actions, I suggest you look it up on the internet and see how it impacts your privacy.

The book's companion website (privacy.clinic) will also have regularly updated information about how to best tweak your browser settings for optimal privacy.

Info

Firefox Lockwise

Firefox Lockwise is a password management tool that helps you generate, store, and autofill passwords using your Firefox browser. Initially named Lockbox, it was first made available as a separate extension in 2018. It was renamed to Firefox Lockwise and integrated with the browser as a core feature replacing the existing Password Manager in version 70.

Since it is a relatively new addition to Firefox at the time of writing this book, the jury is very much out on the security and privacy aspects of Firefox Lockwise. Especially, for those of you who are already using a password manager such as 1Password, LastPass, BitWarden, or similar, I would advise you to continue using them and deactivate Lockwise features, wherever possible.

Here are a few quick steps to ensure that Lockwise does not cause a conflict with your existing password management software.

Click Privacy & Security in the sidebar and, under the section titled Logins and Passwords , uncheck all the checkboxes, viz.

Ask to save logins and passwords for websites

Use a master password

You might also want to separately uncheck the box that says Show alerts about passwords for breached websites . This is a feature allows Lockwise to anonymously track existing breaches, compare your passwords against them, and inform you if any of your passwords have been 'cracked'. 1Password also provides something similar called Watchtower in conjunction with Troy Hunt's Have I Been Pwned service – same as the one used by Lockwise.

Click the Saved Logins button and evaluate the usernames and passwords if already stored by Lockwise.

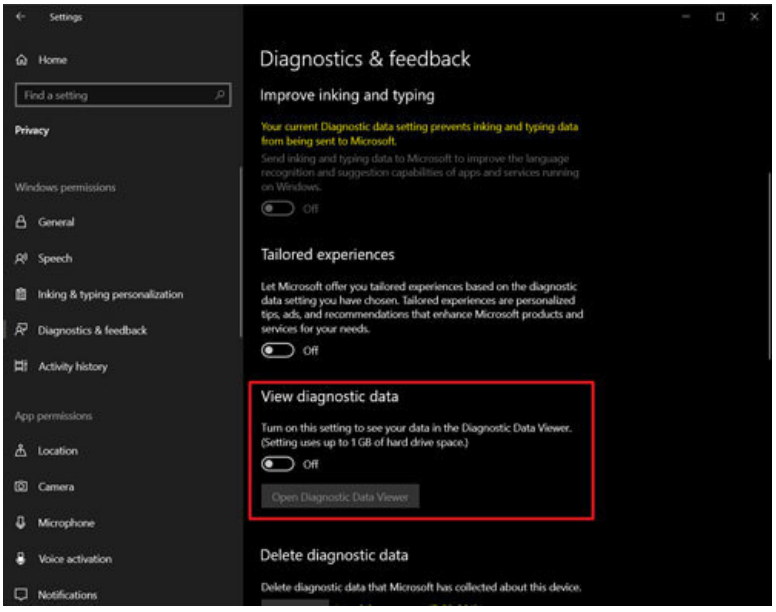


Figure 7.2: The option to turn on Diagnostic Data viewing capabilities in the Diagnostics & feedback section under Settings > Privacy in Windows 10 (v1903)

Note that this will collect and store any diagnostics data collected (upto 1 GB or 30 days, whichever is less) on your PC.

In the next section, which is simply named History , uncheck the box next to Remember to Search and Form History . This will ensure that no form of data gets saved by the browser.

While Firefox Lockwise seems like a useful password management tool, I cannot whole-heartedly recommend it at the moment, since it hasn't undergone the test of time, that is, it hasn't been used by enough users yet. You might want to keep an eye on how things develop over at the companion website, that is, https://privacy.clinic -- scan the QR code given alongside this paragraph and bookmark the page that it opens in your browser.

[QR Code: https://privacy.clinic]

Safari, by Apple

Due to Apple's strong stance on the privacy of user data, Safari does not send any telemetry data back to Apple servers, or provide any syncing and/or personalization options. However, there are a few other settings in your Safari installation that you might want to tweak.

Assuming you are using Safari on macOS, go to Safari | Preferences and follow all of the recommendations listed below:

Default search engines: Choose the Search tab and in the dropdown next to Search Engine , choose a more privacy-aware search engine, such as DuckDuckGo.

Search suggestions: In the Search tab, under the Search Engine dropdown, uncheck the box that says Include search engine suggestions .

Privacy and cookies: In the Privacy tab, check both the checkboxes, under Website tracking , that is,

Prevent cross-site tracking

Ask websites not to track me

Websites: In the Websites tab, you'll find a bunch of options in the sidebar, such as Reader, Content Blockers, Auto-Play, Camera, Microphone, Location, Notifications , and many more. These options correspond to how Safari behaves when it encounters one of these elements on a website visited by you. The default behavior for each of these options can be changed using the corresponding dropdown on the right-hand side.

Autofill: In the Autofill tab, uncheck all four options, that is,

Using information from my contacts

Usernames and passwords

Credit cards

Other forms

Google Chrome

Please refer to the INTERMEDIATE -level recommendations, described further in this chapter.

Keystroke logging

In January 2015, Microsoft announced the availability of an assistant feature named Cortana for Windows 10 desktops and mobile devices. Cortana is an intelligent assistant (similar to Siri and Google Assistant) who learns your behaviors and tailors recommendations and suggestions to match your day-to-day usage and behavior. For this to be made possible, however, Microsoft needs to collect all kinds of data, including but not limited to speech, inking, and typing.

In other words, everything you type, say or draw on a Windows 10 device is available for Microsoft to acquire and analyze. While some may see this as a necessary 'sacrifice' to improve the operating system's capabilities by way of personalization, I see it as excessive sharing of data with Microsoft.

Cortana

Cortana, who derives her name from the famous Halo franchise of games on Xbox, is the name of the digital assistant introduced by Microsoft in January 2015. Since then, Cortana has been integrated into numerous Microsoft's products, such as Microsoft Edge browser, Bing search engine, Band smartwatch, and more.

Info

For people who have installed (or upgraded to) Windows 10 version 1903 or later, Cortana and Search have been split into two separate sections. Cortana and Search both now have their own sections in the Settings screen. I would strongly recommend checking out the various privacy options under each section and toggling any switches that are designed to share your data with unwanted third-parties.

Cortana provides you with a plethora of personalization options through something called the Notebook . To access Cortana's Notebook, open the Cortana app, click on the hamburger menu (that is, the three horizontal lines at the top left) and click the Notebook icon below the Home icon.

Extensions

The extensions that I will be recommending in this section are recommended not just by us but by almost all the privacy and security experts around the world. You can always find the latest set of recommended extensions at https://privacy.clinic/

uBlock Origin [5] : uBlock Origin is a completely open-source extension that touts itself as an efficient wide-spectrum-blocker, that is, it goes above and beyond blocking ads. uBlock Origin uses filter lists constructed and maintained by volunteers to identify and block ads from loading on pages. It is available for both desktop and mobile versions of most major browsers. uBlock Origin consumes very little memory and barely interferes in your internet browsing, except for removing any ads or tracking scripts from the webpage that is being loaded.

Privacy Badger: Privacy Badger is an open-source extension that works along the same lines as uBlock Origin, that is, it stops advertisers and third-party trackers from tracking you across multiple websites without your permission. Created by the Electronic Frontier Foundation, Privacy Badger stops third-party trackers but allows first-party tracking in order to promote a balanced approach to internet privacy between consumers and content providers. It employs a heuristic that only blocks advertisers and tracking cookies that do not respect the Do Not Track setting in a user's web browser.

Info

The ethics of ad-blocking

Sometimes, you might hear an argument about how blocking ads is illegal because it stops content producers from earning money for their content. The emotional appeal of the argument certainly makes people think twice before installing ad blockers. However, there are four much bigger, much more important arguments in favor of ad-blockers:

Malware: Since the early days of the internet, ads have often been used to deploy malware on to unsuspecting users.

Aggressive user profiling: In more recent times, advertising networks aggressively collected tons of user data through the usage of 3rd party cookies, to the point where ads began to feel creepily stalker-ish.

Autoplay ads: Even now, inspite of adblockers gaining rapid popularity, websites and advertisers insist on pushing autoplaying video ads which consume not only unnecessary screen space but also consume costly internet data.

Bloated webpages: The stark difference in page sizes and page load times for most websites with and without ads makes adblocking not just a lucrative option, but a necessary one.

Advertisers and advertising networks have abused consumer trust to a point where ad-blocking is no longer an ethical question but a financial one. In other words, I no longer have any questions about the ethics of using adblockers - I firmly stand in favor of them.

HTTPS everywhere

While most websites have now completely switched over to HTTPS and offer secure browsing for all their webpages, some of them might still use insecure elements on a few pages - wither on purpose, or by accident. The HTTPS Everywhere extension forces the website to use a secure connection (that is, HTTPS) to display all elements on a webpage, thereby ensuring that your browsing experience is made more secure.

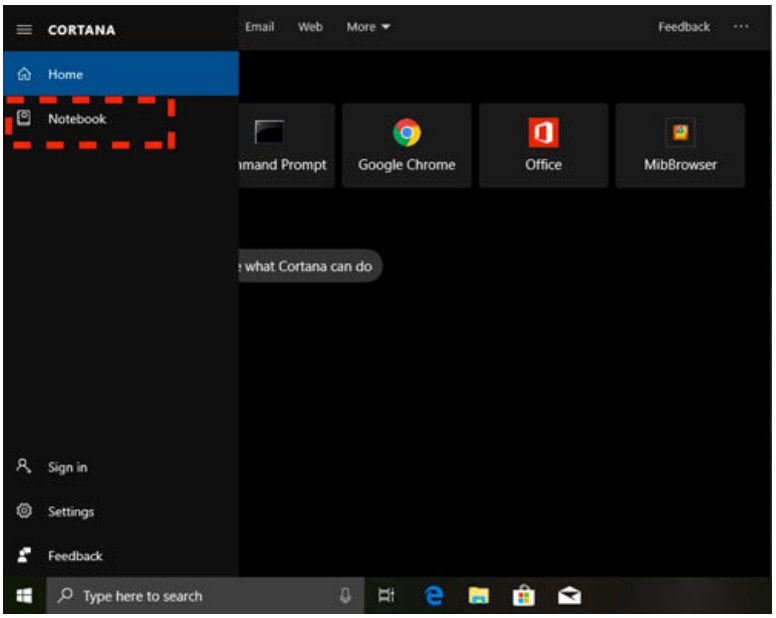


Figure 7.3: Cortana's 'Notebook' can be accessed by clicking the 'hamburger' menu button on the top left.

Here you'll be able to see and edit various personal settings and interests which Cortana will use to personalize your Windows 10 experiences. You'll find that Cortana can acquire information about a wide range of things, starting from your name to the weather in your city, to more intrusive details such as contacts, calendars, and meetings on your schedule.

INTERMEDIATE: (10 points)

Browser recommendation: Same as the recommendations in the BASIC level/section

Private browsing: Same as the recommendations in the BASIC level/section

Privacy settings: I personally believe using Google Chrome is actually detrimental to the privacy of your data. If you insist on using Google Chrome, there are several additional tweaks that you must perform in GoogleChrome settings. That's why I've placed the list of corresponding tweaks to Google Chrome settings under the INTERMEDIATE level of recommendations.

For Google Chrome users, go to Menu | Settings or chrome:\settings and follow all of the recommendations listed below:

Opt-out of telemetry and collection of usage data: In the section titled Sync and Google Services . In the options that are displayed, toggle the following settings off:

Help Improve Chrome Security

Help improve Chrome's features and performance

You may toggle other settings on or off, depending on the level of privacy desired. I recommend leaving Safe Browsing as it prevents you from accessing known malicious sites on the web.

Turn off syncing and personalization: In the section titled Sync and Google Services , toggle the setting titled Do searches and browsing better to OFF . Next, scroll down, open the Advanced Settings , and toggle the Allow Chrome sign-in setting to OFF .

Change your default search engines: In the section titled Search Engine and use the dropdown box to select a different search engine -- I recommend choosing DuckDuckGo instead of Google. If you wish to add a different search engine, simply visit the site or search the internet to find instructions on how to add it.

Search suggestions: In the section titled Sync and Google Services, toggle the setting titled Autocomplete searches and URLs to OFF .

Cookies, tracking, and content blocking: Scroll down to the bottom and click on Advanced to open/unhide the advanced settings. In the section titled Privacy and Security scroll down to Site Settings and click to open it. Under the section titled Permissions , click on Cookies . Among the options displayed underneath, toggle the following settings ON:

Keep local data only until you quit your browser

Block third-party cookies

Ideally, it makes sense to toggle the setting titled Allow sites to save and read cookie data (recommended) to the OFF position, but cookies form an important part of the browsing experience, so I won't recommend turning it off.

Permissions and site-settings: Scroll down and click on Advanced to reveal the hidden settings. In the section titled Privacy and Security , scroll down and open Site Settings . Under the section titled Permissions , you'll find a bunch of options relating to access permissions for the features outlined in the paragraph above. I also recommend toggling all the settings (other than Cookies and JavaScript) to either Ask before accessing or Blocked .

Form autofill: Scroll down to the section titled Autofill and click to open it. You'll find three sections -- Passwords, Payment methods, Addresses.

In the Passwords section, and toggle both the Offer to save passwords and the Auto Sign-in settings to the OFF position. Evaluate and delete any passwords that have already been saved -- both locally and in your Google account -- by performing the appropriate actions in the Saved Passwords section, as and where necessary.

Open the Payment methods section and toggle the Save and fill payment methods setting to the OFF position. Evaluate and delete any payment methods that have already been saved -- both locally and in your Google account -- by performing the appropriate actions in the Payment methods section, as and where necessary.

Open the Addresses and more section and toggle the Save and fill addresses setting to the OFF position. Evaluate and delete any addresses that have already been saved by performing the appropriate actions in the Addresses section, as and where necessary.

Extensions: If all you do on your browser is check your email, share on social networks, and read articles on various websites, then the extensions I am about to recommend are probably not for you. Sure, they might help you with some aspects of your browsing but if you don't know (or can't understand) what the extension does, just skip to the next chapter, directly.

Cookie Auto Delete: The cookies stored by various websites remain on your system until well after you have closed your browser tabs and windows. This is done primarily to ensure trivial conveniences such as not needing to log in the next time you open your browser window. However, it also means that the website that sent you the cookie gets to acquire more information about you and your browsing behaviors. Cookie AutoDelete automatically deletes cookies when you close the tab. Without the cookies, the website cannot recognize you and, therefore, won't be able to create a cumulative profile based on your browsing habits.

Decentraleyes: To save time and bandwidth, websites serve all of their JS/CSS libraries from blazing fast servers called CDNs, or Content Delivery Networks. However, every request made to a CDN server carries quite a bit of information about both, the browser making the request AND the website for which the request was made. CDNs are, therefore, in a unique position to carry out comprehensive user-tracking. The Decentraleyes extension, instead, intercepts the request to the CDNs and serves the requested library from local storage, thereby reducing the possibility of any such tracking by the CDN itself.

Info

Content Delivery Networks

All webpages are primarily comprised of three different kinds of resources -- text, scripts, and objects. Typically, websites rely on JavaScript and CSS to look pretty and perform different actions/animations/functions within the browser itself. There exist several compilations of JS scripts and CSS stylesheets (libraries) that provide lots of different functionalities out-of-the-box. The most commonly used JS and/or CSS libraries are made available through a bunch of fast servers called CDNs , a.k.a. Content Delivery Networks.

Terms of Service; Didn't Read: It is believed that I have read and agree with the Terms & Conditions is the biggest lie on the web -- we often think of it as just another box that needs to be checked to be able to move to the next step. However, this simple action can (and often does) mean signing away significant portions of rights over your own data and your own content. To counter this, a bunch of good samaritans over the internet banded together to create the Terms of Service; Didn't Read (short: ToS;DR) project in 2012. The ToS;DR website (and the ToS;DR add-on, available for most popular browsers) gives short, human-readable summaries of a website's ToS and also grades this ToS on the basis of their impact on the privacy of your data.

Wi-Fi Sense

In a bid to help users connect with wireless networks easily, Microsoft provides a feature called Wi-Fi Sense in older versions of Windows, and this feature can be enabled by default, assuming you don't pay attention to it during Windows installations.

Wi-Fi Sense allowed you to connect automatically to trusted open Wi-Fi hotspots, that is,Wi-Fi hotspots that other Windows 10 users have connected to in the past. If any of these users happened to be a friend (that is, happened to be in your Skype, Outlook, or Facebook contact lists), then you could connect to all Wi-Fi hotspots that were previously connected to by this friend . Wi-Fi Sense was discontinued by Microsoft after it received tremendous backlash from security researchers for ignoring the obvious privacy implications inherent in its design.

Microsoft made this possible by encrypting your Wi-Fi password and storing it on Microsoft servers. I will not debate whether or not Microsoft's servers are secure enough for this action to be considered safe – that's another matter, for another book.

However, consider this scenario: Say, you enable Wi-Fi Sense on your Windows 10 machine. Say, a neighbor in your building happens to be your Facebook friend who also uses Windows 10 and has Wi-Fi Sense enabled on their machine. This means that your neighbor can connect to your Wi-Fi network and vice-versa! Since this applies to ALL your friends on Skype, Outlook, and Facebook, the obvious question is: do you completely trust ALL of your friends on Skype, Outlook, and Facebook? What happens if one of them happens to be an adversary?

The privacy nightmare doesn't end here. Say, you do the responsible, recommended thing and disable Wi-Fi Sense on your Windows 10 machine. At some point, a neighbor asks for your Wi-Fi password and connects with their Windows 10 device with Wi-Fi sense enabled and the 'Share network with my contacts' option enabled. Now all the people in your neighbor's Skype, Outlook, and Facebook contact lists have access to your password-protected Wi-Fi network, even though you explicitly denied Microsoft any access to it!

Forget the privacy and security considerations for a moment and answer just this: In this day and age, do you really want people to be able to access the internet through your Wi-Fi network without your explicit permission or knowledge?

Note

Wi-Fi Sense is Discontinued. NOT!

Although Wi-Fi Sense has been 'discontinued', the option to sync Wi-Fi credentials between machines sharing the same login account still exists. That means, if you log into a new Windows 10 machine using the same Microsoft credentials, then you can 'import' various settings from one machine to the other -- one of which happens to be the Wi-Fi passwords stored on existing machines. As for macOS, a good password manager such as LastPass, Bitwarden, or Keepass works much better than Keychain to manage your passwords.

ADVANCED: (15 points)

Apple's Keychain and 'KeySteal'

Apple also provides a feature similar to Wi-Fi Sense as a part of macOS, called Keychain . Keychain is also available for iOS, that is, Apple iPhones.

Keychain is a macOS application that stores your important private information (such as usernames and passwords for the Safari browser, credit cards, Wi-Fi passwords) on approved devices connected with the same iCloud ID. The problems with the mac OS Keychain are the same as those of Wi-Fi Sense. Furthermore, obvious vulnerability notwithstanding, Keychain has also been shown to be vulnerable on multiple occasions by multiple researchers.

In 2017, an information security researcher tweeted an exploit for Keychain that could extract stored passwords in plaintext. This exploit was immediately patched by Apple in the macOS High Sierra 10.13 supplemental update. In February 2019, a German researcher discovered the KeySteal vulnerability in macOS Mojave 10.14 through a different exploit that could be used to extract all the data stored in the Keychain by installing a hidden malware. Apple patched this vulnerability in a subsequent update, but Keychain continues to remain a lucrative target for many more exploits in the future.

Browser recommendation

There are three things I would specifically recommend for advanced users:

Use Firefox. Uninstall all the other browsers.

Use Firefox's private windows for any and all casual surfing.

Use the Tor browser for all your private and/or anonymous actions.

Do not mix any of the above three use-cases EVER.

Other privacy settings

As of July 2019, the latest update of Windows 10 (version 1903) still had a few data-sharing settings that could be construed as significant privacy concerns. Primary among these was the unique advertising ID allocated to each Windows 10 machine, at the time of installation. You can find this in the General section of the Privacy category in the Settings app, which can be found in the sidebar. There are a total of four major sections in the sidebar:

General

Speech, inking, and typing

Diagnostics and feedback

Activity History

In some cases, sharing this data can help personalize the various recommendations and suggestions you see on your Windows 10 device. However, from the perspective of minimizing data-sharing with third parties, I recommend that you toggle *all* the data-sharing switches to the OFF position for each of the sections. I also recommend that you ensure that any data stored by Windows 10 (whether on your device or in the cloud) is immediately cleared.

Scrolling down further you'll notice a section titled App Permissions under which are listed various hardware devices and services (for example, Location, Camera, Microphone, and many more) which collect your data and share with Microsoft servers when toggled on.

Private browsing

See recommendation above.

RohitRecommends

Almost all of my recommendations in this section will be aimed at Windows 10 users.

Why? Because there isn't much to recommend for either Apple or Linux users! Both these operating systems have rather robust (and a pretty straightforward) philosophy about maintaining the privacy of user data. Furthermore, both these operating systems provide simple and straightforward opt-out methods for users who do not wish to participate in sharing any telemetry data from their devices.

Privacy settings

One of the quickest ways to create a robust set of privacy-aware settings for Firefox is a service called Firefox Profilemaker . It is made by a GitHub user named allo- and can be accessed at ffprofile.com . The website takes you through a bunch of questions that will evaluate your privacy requirements and generate a Firefox profile specific to your needs. The site also provides detailed instructions [6] on how to 'install' this profile, at the end of the process.

If you decide to replace your existing Firefox profile, I strongly recommend that you first back up the existing profile folder before you proceed with the steps detailed by ffprofile.com . Scan the QR code given alongside to open the Firefox Profilemaker on your device.

[QR Code: https://ffprofile.com]

Operating system (OS)

The choice of your operating system will determine which of the recommendations you will need to follow from this section. Simply put, I have assumed the following to be true:

You are a Windows user. Given that almost 90% of Indians use some version of Windows as their operating system; this isn't a very far-fetched assumption.

You haven't really paid attention to what Windows does with your usage data.

You are running a clean install of the latest version [6] of Windows 10 OS.

Windows is known to collect data from its users aggressively. On the other hand, macOS (and Apple) have openly proclaimed, on multiple occasions that they always choose to put the user's privacy ahead of everything else.

Since most Linux distributions are open-source and (mostly) community-driven, collection of user data is actively discouraged. That said, Linux distributions that are developed by specific organizations such as Canonical or Endless may collect some kind of telemetry data, but they usually provide an easy and straightforward way to opt-out of such data collection as well.

Thus, the recommendations that I have made in the following section are primarily based on three main criteria:

Desire to switch

Ease of use

Ease of switch

My recommendations for an ideal operating system are primarily based on whether or not you are open to switching to a new operating system -- everything else follows from there. If you are open to switching, then I'll evaluate and recommend an alternative OS that is relatively easy to use for your specific use-case.

Extensions

uMatrix: uMatrix is an extension for advanced users, which provides a point-and-click blocker philosophy and interface (almost like a firewall) for each webpage you browse. According to the developer, uMatrix puts you in full control of where your browser is allowed to connect, what type of data it is allowed to download, and what it is allowed to execute.

Upon installation, uMatrix works in a block-all, allow exceptionally mode, that is, it blocks all 3rd-party scripts from being loaded in the browser. This is likely to break quite a few web-pages, so make sure you know what you are doing.

Firefox multi-account containers extension: Recently, Firefox included a unique feature called multi-account containers to its browser. Multi-account containers allow you to separate your personal, work, shopping, etc. identities without having to log out each time. Each container has separate access to a different part of the browser's storage, which means that all your site-specific preferences, cookies, and tracking data (if any) are associated with the container, rather than the entire browser.

Multi-account containers are a simple and quick method to login (and stay logged in) to several accounts at once without any account interfering with any of the others. This is useful if you created different accounts for your work and personal needs.

Facebook container: The Facebook container is a highly-specialized version of multi-account container that isolates all links related to Facebook (and associated websites such as Instagram, Messenger, and many more) in a separate container. If a website opened in another container happens to include an element from Facebook (for example, the like button), the element itself is invoked in the Facebook container due to the strict policy of the extension.

Thus, any and all cookies set by Facebook (and associated websites) are isolated and your regular browsing stays untracked .

BASIC: (1 point)

Important!!

I do not recommend using any version of Windows older than Windows 10.

I'll say that again: I absolutely do NOT recommend using any version of Windows older than Windows 10.

That means anyone using a version of Windows that is not Windows 10 (such as Windows 7, Vista, XP, or lower) must upgrade immediately to Windows 10, preferably the latest update made available by Microsoft [7] . The support lifecycle for all other versions of Windows has either ended or will end soon. The wide variety of vulnerabilities that have since been discovered and distributed may render your computer susceptible to various penetrative attacks by adverse actors.

In other words, if you are still running an older version of Windows, you are very likely to get hacked and/or your data stolen, and there's not much I (or anyone) can do to help unless you choose to upgrade your OS to the latest available version of Windows 10.

If you feel you are comfortable with Windows as your primary operating system aren't looking to change, then I strongly recommend that you do the following, at the very least:

Upgrade your Windows to the latest version: As of the date this chapter was written, this happens to be Windows 10, build 1903. If you are using Windows 8, or 8.1, upgrade to Windows 10 as soon as you can. Windows 7 users had until January 14, 2020, to upgrade and I strongly recommend that you upgrade to Windows 10 and get used to the (somewhat) different interface and OS behavior.

Update all programs to their latest version: While Microsoft automatically pushes various updates and patches continuously to ensure that your Windows is protected from various vulnerabilities, it is your responsibility to ensure that you do the same for the various third-party software that is installed on your system. An attacker trying to steal your private information will often try and exploit known vulnerabilities in such software to gain unauthorized access to your system.

Encrypt your data: For users with newer machines, I strongly recommend using encryption software to encrypt files on your system. If you are running the Ultimate or Enterprise versions of Windows, you can use the built-in tool named BitLocker, or you can use third-party tools such as

TrueCrypt or VeraCrypt to encrypt your system

Maintain multiple backups and redundancy of data: Not matter how careful you are; there is always a chance something goes wrong. To protect yourself from mishaps, always maintain multiple copies of your most important documents and files. I always recommend maintaining at least three copies – one master copy, one in an external drive, and one online. Keep all three copies constantly in sync so that you can get back up and running should something somehow go wrong with your master copy.

Follow the various recommendations given across the book: Windows is the OS of choice for many Indians, and it is a tough ask to move from something they have (probably) used for almost their entire life. So, if you insist on continuing to use Windows, ensure that you follow the various recommendations given across this book, specifically this chapter. You must pay special attention to the parts on OS Telemetry and Bloatware.

This is the absolute bare minimum I recommend for any Windows system.

EXPERT: (25 points)

At this level [7] , you probably want to avoid all other browsers and just use the Tor browser inconjunction with software and services that promise similar or better levels of privacy and anonymity, such as the .onion network, Tor-compatible VPNs, anonymous file-drop services, and so on.

Important!!

I do not recommend using this for casual internet browsing at all! Reserve your Tor browser usage for when something serious is at stake.

While Tor traffic is known to be highly secure, extremely anonymous, and difficult to decrypt, it certainly is closely monitored by several entities -- state and non-state actors.

INTERMEDIATE: (2 points)

If you have the resources (financial, mental, as well as time) to spare, I strongly recommend switching to a more secure and more privacy-aware operating system such as macOS and/or a Linux distribution that works for you. Both these operating systems are built on the promise of user-privacy and known to keep user interests front-and-center with each of their major updates.

I understand that switching to a Mac will be expensive while switching to Linux is sure to be time-consuming -- I absolutely don't recommend doing either on a lark. In fact, I recommend doing this only after you have thoroughly evaluated your privacy requirements and are absolutely sure that you can afford it -- financially, mentally, and only if you have ample time to spare.

ADVANCED: (3 points)

For those who are paranoid about their privacy and security, I recommend doing one (or both) of the following things:

Installing Tor

A combination of operating systems by running one inside the other using a VM. For instance, the most common example is to run a privacy-focused Linux distro such as Whonix as a VM on a suitable host system. Ideally, having a privacy-aware OS (that is, macOS or a suitable Linux distro) for a host is recommended.

Download the Tor Browser Bundle, and extract it to a folder of your choice. Double-click the icon named Start Tor Browser and wait for it to establish the relay. A short while later, the Tor browser window will open and you will see the standard Tor connection message. That's it, you're done! You can now access any website on the internet with the highest level of privacy and under maximum anonymity.

Always carry a bootable Live USB of a privacy-aware OS , such as Tails, Discreete, and many more. In case you absolutely need to access the internet using a semi-private or public machine, use this bootable USB to boot into the Live OS and access your data securely.

Personally, I carry a bootable Live USB with Tails installed on it everywhere I go. It comes in very handy when I need to use unknown computers.

EXPERT: (5 points)

The configurations described under the previous level (that is, Advanced) will ensure that you don't accidentally leak your own data in a semi-private or public setting.

However, for users who want their privacy to be maintained in all scenarios need configurations that are more secure and more private than this. There are multiple ways to achieve this, all of which are mostly custom configurations designed for specific use-cases. Each one of them involves designing a specific (somewhat-complex) configuration that is rather unique to the requirements postulated by the user.

Using Tor

There are a few things to keep in mind while using Tor:

Use the Tor browser as-is -- do NOT change anything!: Although the Tor browser is basically a modified version of the Firefox browser, it is designed and constructed with specific settings to confound browser fingerprinting techniques, thereby ensuring maximum anonymity. If you change any settings, you are likely to change the fingerprint generated by your Tor browser, which could potentially unmask your presence. In simple words:

1) Do not install or remove any extensions

2) Do not change any settings

3) Do not even maximize the window, or change the size/shape of the window in any way, shape, or form.

Do not log in to any websites while using Tor: Although most popular websites on the internet now recognize Tor relays and make adequate provisions, there is always the chance that the automated spam filter might flag you as a bot or, worse, a malicious actor and lock you out of your account. Moreover, logging into an account means identifying yourself to a website with a username and password combination, which basically defeats the whole purpose of using Tor to become anonymous!

Choose Tor-friendly, privacy-aware services in conjunction with the Tor browser: I've already mentioned how Windows does not have a great track record in terms of privacy and security of the end user. If your Windows login is somehow compromised, there is every possibility that your Tor browsing may also end up being compromised. Hence, I strongly recommend that you use Tor in conjunction with a privacy-aware OS such as Tails or Whonix, whenever possible.

The same argument also applies to your browsing habits, incidentally. Most websites attempt to track you and generate a unique profile ID by default. They will then track you across the web using this profile ID and associate every action you take with this profile ID. While Tor tries to ensure that no cookies can be associated with your real identity, there are chances that you may slip up and reveal you're true identity somewhere. Choose privacy-aware options to your usual websites, for example, DuckDuckGo instead of Google, Protonmail instead of Gmail, Signal instead of WhatsApp, and many more.

Use Tor liberally, but carefully and responsibly: Tor works under the assumption that if everyone appears the same to an observer, then no one has a unique identity, therefore everyone is anonymous. This is why Tor attempts to create a uniform identity for everyone who uses Tor. Thus, every time you use Tor, you add another faceless identity to the crowd which can be extremely helpful for someone who needs it, for example, people trying to communicate in oppressive regimes, or whistle-blowers trying to get the message out.

Spy vs spy!

In one specific case, I was asked by a client to design a configuration that would leave little to no trace of identifying data if it were to be accessed from a random public computer, such as the one available in a library. This was a client working with intelligence agencies and needed to ensure that their browsing habits would not accidentally give away details about themselves.

This case was particularly challenging because operating systems often keep track of the timestamps when plug-and-play devices are plugged in and/or removed. Without administrative privileges, it would be difficult to remove any record of this data stored by the host system. Couple that, with the general surveillance options available to their adversaries, it was imperative that the client could access computers and leave no trace behind.

We, therefore, settled on creating a bootable USB with a slightly customized version of the TAILS distro, with a few additional persistent software, viz. a secure VPN, a secure messaging app, a disk-encryption tool, among other things.

The client was advised to tunnel into the TOR service through a VPN to ensure double redundancy and was strictly told to avoid frivolous browsing and/or logging into any websites on the internet. Their email service was moved to a more secure option, and all file-uploads were routed to more secure file-drop servers. Any messaging with the necessary agencies was either ephemeral or carried out over messaging apps with 2048-bit end-to-end encryption.

Although the client was mostly a Windows user, they managed to understand the new environment quite easily and were able to adjust their digital behavior and ensure maximum privacy and security, using the detailed steps that I had outlined for them.

Caveat Emp-tor!

[8]

While the Tor browser is a quick-and-easy option for surfing the internet anonymously, one must remember that it works on the principle of building multiple relays between your browser and the remote server. That means your traffic could very well be intercepted by an adversary. (See the section on Tor Browsers earlier in the chapter for a slightly more detailed explanation.).

Although all Tor traffic is encrypted, there is always a possibility that a dedicated adversary could find ways to compromise your system, your anonymity, and expose your identity. Or simply, there may arise certain situations where you require a higher grade of anonymity and privacy than what Tor has to offer. For instance, you may be a celebrity wishing to maintain anonymity in the digital world. Or you may be someone who needs to fly under the radar for reasons involving harassment, bullying, or something similar. There is a multitude of reasons why you might need such a customized solution.

In such situations, I recommend a customized approach, tailored to your specific needs, to maintaining your privacy, the details of which are rather complicated to explain in this guide. I recommend you consult with experts on how best to achieve this for your specific case. You can also refer to the companion website, that is, https://www.privacy.clinic , where you can find detailed articles and casestudies, published from time-to-time, describing how I was able to achieve better anonymity by customizing solutions for our clients in specific scenarios.

Telemetry

If you are worried about the amount of telemetry data collected by Microsoft servers, then there is a solution to ease your worries. Thankfully, in most of these cases, Microsoft has provided an option to turn off the sharing of such data (for what it's worth) by toggling the appropriate switches in the OS settings -- all of them bundled under a single heading called Privacy .

Regardless of what you ultimately choose to do with the data that your Windows machine is sharing with Microsoft servers, you need to aware of the scope and extent of data being collected under the Diagnostics and Feedback section under Settings . For purposes of this section, award yourself 1 point.

Let's look at some of the most crucial sections under the Privacy section in the Settings app.

Conclusion

In my personal opinion, Google (and its parent company Alphabet) cannot be completely trusted to be privacy-focused. Their entire business model revolves around finding the right customers for the right advertisers and vice-versa.

That would be like asking a wolf to guard the sheep, wouldn't it?

And I do not voice these concerns lightly; Google has given us several reasons over the years to be distrustful of them. For example, in 2018, Chrome introduced a feature that caused users signed into any Google service to be automatically signed in to their Chrome browser as well. Google insisted (and continues to insist) that this doesn't change any existing data-collection policies, but given how extensive and exhaustive their existing data-collection policies already are, I'm not sure how much of a difference this assurance actually makes.

If all that has got you wondering, which of the popular browsers available today qualifies as privacy-focused, prepare to be somewhat disappointed.

Although both Mozilla Firefox and Safari claim that they are considerate of your privacy, they are privacy-aware rather than privacy-focused, at best. Brave is still a relatively new (and therefore unknown) entity, in spite of all its brave words. Using Tor to access your email and social networks is comparable to using a hammer for etching your name on a grain of rice.

Then there are the other questions:

Does tweaking your browser settings provide enough cover to protect the privacy of your personal data?

Won't the websites you visit continue to store your data long after you close your browser window?

Can you control what these websites choose to do with your data?

And exactly that's what we'll be discussing in the subsequent chapters -- services and networks. Get ready!

---

[1] You'd be surprised by the amount of resistance it can generate if you ask people to switch to a different browser - even if the only change involved requires clicking a different-looking icon.

[2] I would have recommended StartPage but in the time it took me to finish the manuscript for this book, System1 invested in StartPage through one of their subsidiaries called Privacy One. System1 is an advertising company.

[3] Personally, I prefer Mozilla Firefox. I'm not yet entirely clear about Brave's intentions…

[4] Don't worry, if something goes wrong, you can always start with a fresh browser 'profile'.

[5] uBlock Origin and uBlock are DIFFERENT extensions. uBlock Origin was forked from uBlock by the original developer because of shady

practices by the maintainer. Make sure you install “uBlock Origin”, and NOT “uBlock”.

[6] If you decide to replace your existing Firefox profile, I strongly recommend that you first back up the existing profile folder before you proceed with the steps detailed by ffprofile.com.

[7] I do not recommend using this for casual internet browsing at all! Reserve your Tor browser usage for when something serious is at stake. While Tor traffic cannot be easily decrypted, it certainly is closely monitored by several entities -- state and non-state actors.

[8] That’s Latin for "Buyer beware!"

Diagnostics & feedback

Windows 10 users on the Pro, Enterprise, or Server versions have an option to switch off the collection of diagnostic data completely. Unfortunately, for users running the Windows Home version, this collection of data cannot be completely stopped but can only be restricted to a certain degree.

Chapter 10

Services - Email

Keystroke logging

First, go to the Speech, inking, & typing section under Privacy in the Settings app and click on the toggle switch next to Turn off speech services and typing suggestions . You'll still be able to use Windows Speech Recognition to some extent, but it won't be able to learn from you.

Introduction

Whenever someone says they did something on the internet, for example, bought a dress, posted a comment or an update, uploaded a photo, checked out a website, what do they actually mean? How actually does doing something on the internet work?

Broadly, the process of ‘doing something on the internet' can be divided into three parts:

Using an internet-capable device, such as a laptop or a smartphone.

Connecting via an internet service provider, or ISP.

Accessing a service (that is, using a website) over the internet connection.

When you think about it, each one of these three parts contains information relevant (and maybe, critical) to you and your identity. Your device stores information about you. Your ISP provides the infrastructure that carries the information you send to remote servers. The services you access receive (and often, store) the information you send for processing and analysis. Also, each of these three parts, if intercepted by someone, can cause your information to be leaked.

That's why it is important to secure each of these three parts as much as possible.

In the previous chapter, we have already discussed ensuring that the first part, that is, your devices are secured, in quite a bit of detail. I'll be dedicating this section to ensuring that we do the same for the other two. I'll start by looking at some of the most frequently used services on the internet and how to go about securing them, such that they leak as little information about you as is possible. Specifically, I'll be talking about your email, social networks, shopping, banking, and general online behaviors and how to make them secure.

Email

The email was one of the first services to be introduced on the internet, and it still constitutes a major portion of the daily traffic on the web. In fact, according to a recent report by Radicati, there are over 3.9 billion email users worldwide, and they send around 293 billion emails per day. That's a little under one hundred emails sent per user on average.

Cortana

Not many Indians are power users of the Windows operating system, that is, we do not rely on digital assistants to organize our day-to-day tasks and schedules. Therefore, I strongly recommend that you turn Cortana off entirely. Not being able to use Cortana won't make a noticeable difference in your Windows experience but turning Cortana off is likely to mitigate some privacy concerns, for sure certainly.

Info

This does not stop Windows 10 from reporting your search back to Microsoft, as ArsTechnica recently found out. The QR code given alongside

this paragraph points to the ArsTechnica article, “Even when told not to, Windows 10 just can't stop talking to Microsoft.” Note that the article is from 2015, so some portions of the article may no longer be relevant.

[QR Code: https://www.radicati.com/wp/wp-content/uploads/2019/04/Email-Market-2019-2023-Executive-Summary.pdf]

One could make the argument that, due to the growth of instant messaging solutions, the total number of email users is likely to have decreased somewhat over the years. However, email definitely continues to be one of the preferred modes of communication, especially among corporate users.

Emails also constitute a valid form of identity over the internet with a large number of websites choosing to let users supply their email ids as logins, instead of creating separate usernames.

[QR Code: https://arstechnica.com/information-technology/2015/08/even-when-told-not-to-windows-10-just-cant-stop-talking-to-microsoft/]

Accessing email

There are two distinct people access to email in one of two ways:

Online: By logging in to the email web portal in your browser.

Offline: By logging in through an application (for example, an email client) on your device.

As is obvious, each method has its own pros and cons and its own set of dos and don'ts, which I'll outline one-by-one in the #RohitRecommends section of this chapter.

Wi-Fi Sense

I recommend that you toggle Wi-Fi Sense OFF on your Windows 10 device. I also recommend that you do not share your Wi-Fi password with anyone -- not even your loved ones, not unless they are reading (or have already read) this book!

Web-based portals

The practice of storing emails locally using an email client has clear and major privacy implications. Specifically, it violates the first guiding principle of privacy mentioned in the very first chapter. In this regard, web-based portals score over email clients due to their on-demand nature, that is, they only display email that you request.

Web-based portals are preferred by people who need to access their emails from different devices at different times. Although email apps on the smartphone have replaced browsers for this specific need, there may still be instances where logging into your account using a browser may be preferred.

Other 'Privacy' Settings

I recommend that you drill down into each one of these device options (or service options) in the sidebar, and toggle the various switches to the OFF position, depending on your comfort with the amount of data available and shared by each of them.

Specifically, if you own a laptop or have a webcam attached to your Windows 10 machine, ensure that you evaluate the privacy settings for the following sections in the sidebar:

Location

Camera

Microphone

Voice Activation

You might also want to look at all of the remaining settings and make of note of which programs have been provided access to which data on your device. If an app seems even slightly suspicious, toggle the corresponding switch to the OFF position. Better safe than sorry!

Info

OOSU 10

There is a third-party portable freeware called OOSU 10 (short for O&O Shut Up) which provides you with a single interface for toggling the various data-sharing options in Windows 10. It doesn't need to be installed and can be run from anywhere on your PC -- even a flash drive. You can download it here: O&O Shut Up10.

Email clients

Email clients work slightly differently from web-based portals in that they require you to provide your access credentials only once -- usually during setup.

Once the email server authenticates the login credentials and authorizes the client, the client downloads emails from the server at regular interval using the login credentials already supplied. These emails are stored locally on the device, as opposed to retrieving them from a remote server on demand, in the case of web-based portals.

[QR Code: https://www.oo-software.com/en/shutup10]

However, the chances are that you won't need to do much here. One, most of the software that we use on Windows doesn't really make much use of these permissions. Two, the small number of apps that do end up using these permissions are usually ones downloaded from the official Microsoft store and therefore, mostly legit.

Personally, I have completely switched off app-access to all of the features listed in the sidebar (and not just the four named above) on all my Windows devices. None of the software installed on my machine uses this permissions framework, and the apps that do use this framework aren't of much use to me.

That being said, it doesn't hurt (and most certainly helps) to keep checking these permissions from time-to-time, to see if there are any unwanted apps that might be abusing any permissions, either accidentally or maliciously.

Compromising your email

The process of compromising an email account is a lot simpler than it seems but a lot more difficult than most people are led tobelieve. Unlike the myths made popular by several movies and TV series, malicious actors do not spend their time trying to figure out passwords letter-by-letter.

Instead, they use a variety of different techniques to infiltrate your email account and/or your device then and access crucial data from within. I'll outline some of the most common methods used by malicious actors so that you are aware of what to expect. Later, in the #RohitRecommends section, I will provide concrete steps on how to prevent and/or mitigate these threats and ensure that your email account stays as secure and private as possible.

BASIC: (1 point)

Award yourself TOTAL of ONE point if you only read through all the recommendations made in this section

Phishing

The technique of impersonating a friendly contact to elicit sensitive information from a target/victim is called phishing and it is a common method used by attackers to compromise email accounts. It works like this:

An attacker crafts and sends a fake email with language and content designed to look like it could have been written by someone you know. The subject line is usually something simple and generic like, Read this and tell me what you think. or You'll love watching this!

When you click the link to the attachment, a webpage opens up requiring you to log in to your email account to read/view/listen to the attachment. This webpage is always fake and can be identified as fake by looking at the URL in the address bar. For instance, instead of saying google.com, it might say google.com or google.com.update.securesite.app.site –note that neither of these is the official Google website address.

If someone (for example, johnsmith@gmail.com) actually enters their credentials on the fake webpage, their credentials are captured, and the victim is redirected to the actual login page for their email, leaving them none the wiser.

Using the credentials acquired in the previous step, the attacker takes over the inbox of the victim (johnsmith@gmail.com) and sends out mass emails to everyone in the address book. With the same content and fake attachment used in step 1.

This time, however, the email has legitimacy since it is sent using johnsmith@gmail.com's email account. The percentage of people who will click the link and enter their login credentials is likely to be higher, resulting in the attacker being able to capture even more credentials.

INTERMEDIATE: (2 points)

Award yourself TOTAL of TWO points if you followed all the recommendations made in this section.

Weak passwords

Numerous internet security firms have examined and analyzed the millions of passwords leaked in various data breaches. Almost all of them agree that the most common password used by people is: 123456 . The second most common password is usually either password or 123456789 .

We often overestimate our ability to make up good passwords. We often tell ourselves that coming up with secure passwords is easy. In fact, some websites on the internet also claim to provide useful techniques to generate secure-yet-memorable passwords, such as:

Sentence abbreviation: I know what you did last summer!! can be written as !kWyDL5!! which is a somewhat strong password.

The XKCD technique: First suggested by popular comic xkcd.com, it involves combining four common unrelated words such as CorrectHorseBatteryStaple to form one secure password.

Mnemonic devices: For each account, imagine an unlikely scenario and make a mnemonic device, for example, for your Gmail, think of a Shark riding a Pineapple on NH7, and combine them to create GmSh4rN3aPnh7!

Language-mixing: This only works for non-English languages that use an alphabet/script different than the Roman alphabet. Writing native words in the Roman alphabet/script (for example, 2Aankhen12Haath?!) can qualify as a pretty secure password under most circumstances.

Note

If you haven't seen it yet, scan the QR code given alongside to open the specific XKCD comic that first suggested/presented the technique.

Interestingly, the specific password given as an example in the XKCD technique (that is, CorrectHorseBatteryStaple) is not so secure anymore and has already been cracked, according to the Have I Been Pwned database. I definitely do NOT recommend using CorrectHorseBatteryStaple as a password for any of your accounts!

macOS

[QR code: https://www.xkcd.com/936/]

BASIC (1 point)

Apple provides a bunch of configuration options to ensure the privacy of (most of) your data under the System Preferences application in macOS. The System Preferences can be accessed from the gears icon in the dock, or by going via the Apple menu | Preferences .

Click the icon labelled Security & Privacy and scroll through each section to understand how Apple collects and shares data from the various parts of your device. Pay special attention to the tab labelled Privacy and make a note of which apps have been given access to which of your personal information.

Next, you have a decision to make.

Malware

An attacker with access to your email account can craft specific emails (see the additional information box for Phishing) that are designed to infect your system with specific malware, by sending them disguised as harmless attachments.

Many victims have believed outright lies such as, Oh, don't worry, go ahead and click 'Install' on that attachment. I assure you it is completely harmless! simply because the attacker replied from the compromised email account.

Once the victim installs the malware, the attacker gains access to a lot more than just the email accounts. For example, the attacker may install a keylogger that makes it possible for the attacker to intercept *everything* you type, or view, or download, or install - pretty much everything you do on your system.

Thankfully, most antivirus and antimalware software are advanced enough to detect these kinds of intrusions but requires scanning your attachments for virus and malware before you open them.

INTERMEDIATE (2 points)

Once you have checked out all the sections under Security & Privacy in the System Preferences of macOS, toggle relevant switches as and where necessary, depending on the extent of Privacy you would like to maintain.

There may be some instance where you might need to leave a switch toggled on. For instance, sharing the contacts permission with the Spotlight feature may be necessary if you regularly rely on Spotlight to search through your contacts. However, at the same time, you might want to restrict Facebook from accessing the contacts on your macOS.

Check/uncheck the relevant checkbox to grant or deny permissions to the relevant services/features.

Email ads

We've now gotten so used to seeing ads in our email inbox that we don't even stop to consider for a moment how they got there. More often than not, these ads seem to be precisely targeted, highly relevant to our immediate needs. The pin-point accuracy of such ads raises the question, "Is someone reading my emails?"

Sadly, the answer is, Yes .

Your email service provider can 'read' your emails, in the sense that they can process the content of your emails, extract the relevant keywords, identify products that correspond to those keywords, and serve ads for these products directly into your inbox. If you use a web-based portal, these ads may appear as banners, or contextual links, or a specially positioned email, or any other variety of sponsored listing . If you use an offline client, these may take on the appearance of a regular email mixed between your other emails.

Every email service provider who offers free email services scans all your emails and harvests them for useful keywords. The only way you can prevent your private emails from being read is either:

Hosting your own email server

Using a privacy-aware email service provider

Let's take a look at both of these options in a little more detail.

EXPERT (5 points)

Scan the QR code given alongside this paragraph to be taken to an extremely detailed guide about macOS privacy and security is available on this GitHub page compiled by a GitHub user named DrDuh .

Hosting your own email server

This option requires substantial and expert knowledge of email technologies. You will have to ensure that:

You own and maintain your own domain and mail-server.

Your domain and mail-server are always white-listed.

Your server is always secure.

Your inbox is free of spam.

Emails coming to (or sent from) your mail-server don't bounce.

The software running the email server is maintained and up-to-date.

…among many other things. Clearly, this option gives you complete control over your own data but requires you to be completely hands-on.

[QR Code: https://github.com/drduh/macOS-Security-and-Privacy-Guide]

Be warned though, the guide is aimed at power users of mac OS, and it expects you execute console commands as a superuser. While I (and many other privacy experts and enthusiasts) find recommendations given in this guide to be quite useful, my lawyers insist I issue this explicit warning to you, dear reader:

“If you wish to follow the recommendations made in DrDuh's guide, please make sure you do so under expert supervision and know that you'll be doing so at your own risk!”

Linux

Linux is generally considered a highly privacy-aware (if not privacy-focused) operating system. Most Linux distributions usually transmit little to no telemetry data from your devices.

However, a recent case has forced long-time Linux enthusiasts to question this belief.

Around three years ago, in late 2014, users of Ubuntu were surprised to discover that searches performed using the Unity Dash (a search bar built into the Ubuntu Desktop Manager) would return results featuring products you could buy from Amazon. At the time, Canonical categorically stated that all search queries were routed through Canonical's servers to Amazon and other search partners, and not directly as was being assumed.

In light of the controversy that followed, Ubuntu first resisted and finally relented by redesigning the search feature in Unity dash to make it separate and configurable, that is, searches in Unity dash would remain on the local system, and any external search capabilities would have to be 'installed' as plugins to be made available to the users.

Using a privacy-aware email service provider

Let's be honest; option one might not be everyone's cup of tea. That's why option two, that is, using a privacy-aware email service provider, is probably a better option for those who wish to ensure the privacy of their data but aren't looking to invest too much of their time and other resources into maintaining their own email server.

There are several email providers who provide privately-hosted email services. Some of them provide a free account, but most of them offer paid plans. Some of them even offer end-to-end encryption, i.e. emails sent from your inbox are encrypted before they are sent and, therefore, can only be decrypted by the intended recipient.

Some of the most popular examples in this category are ProtonMail, Fastmail, Hushmail, and many more. While Google claims that they do not scan the emails for personalized advertising, they do scan your emails to provide you other related services such as relevant search, integrations with other Google services, providing intelligent features.

Spam

Ongoing research by Valimail indicates that at least 3.4 billion fake emails are sent every day. Another research puts the number for spam email much higher -- at 14.5 billion emails per day. In other words, spam contributes to about 45% of all email traffic.

BASIC (1 point)

Among the popular Linux distributions, Ubuntu is known to collect and transmit some telemetry data back to its servers through the following packages and/or (associated) services:

ubuntu-report: Collects and reports information back to Ubuntu [8] at the end of OS installation.

popcorn: A package that tracks the relative popularity of apps and packages installed by other Ubuntu users.

apport: A package that automatically sends anonymous crash reports back to Ubuntu.

whoopsie: A package that sends the crash reports generated by apport to Ubuntu, but only with your explicit permission.

[QR code: https://www.valimail.com/press/more-than-3-billion-fake-emails-are-sent-worldwide-every-day-valimail-report-finds/]

Identifying and isolating spam emails is an important task that needs to be performed regularly to ensure that you do not get overwhelmed by it.

However, this is easier said than done. The popularity of email as a login identity means that several websites and services across the internet are in possession of your email and will use this information to send unsolicited promotional material to your email inbox. Therefore, it becomes incredibly important to identify and isolate spam before it floods your inbox.

Don't get me wrong; spam by itself does not pose a threat to your privacy or security of your email account. However, an inbox flooded with spam becomes pretty much unusable if the spam continues to pile up. Legitimate emails may get drowned in spam and may cause loss of valuable business and income.

In 2012, it was estimated that spam cost businesses about $20.5 billion per year – a number that was expected to grow to $257 billion per year by 2018.

That's why I always insist that you should have a separate email address to signup for all the unimportant stuff. There are also several other options that you can use to ensure the privacy and security of your inbox, which I will discuss shortly in the relevant section of #RohitRecommends .

ADVANCED (3 points)

If you are an Ubuntu user, search the internet on how to remove the following Ubuntu packages. There are several articles explaining what each of the packages does and how you can safely prevent them from conducting any telemetry.

However, if you are absolutely sure you want to remove them from your Ubuntu system, and if you are comfortable running commands in a terminal, you can simply run the following apt command to remove all packages from your Ubuntu installation:

$ sudo apt purge ubuntu-report popularity-contest apport whoopsie

Additionally, you can block access to metrics.ubuntu.com and popcon.ubuntu.com using the inbuilt firewall or any other firewall of your choice.

RohitRecommends

The first question I ask all my clients, who come to me for consultation, is this:

“If, right this very moment, your email credentials (i.e. your login and password) were to fall in an adversary's hands, how bad would it be?”

99 times out of 100, the answer inevitably is some variation of, Very, VERY bad!

We all have things in our email inbox that we don't want the world to see. Any adversary gaining access to your email inbox will probably end up getting access to not only your personal conversations, but also your financial information, your social media accounts, and a bunch of other online identities. Very few people keep a zero-inbox policy and clear everything out of their inboxes.

Don't get me wrong; I am not advocating a rigorous zero-inbox policy; I understand that it is sometimes useful to have important emails stored in your inbox. We also have to acknowledge the flip side, though -- as long as those emails remain in your inbox, there is always a possibility that someone might be able to access them, without your knowledge or consent.

Conclusion

Just like with smartphones, computers are also usually identified by the operating systems that run them. Broadly speaking, you are likely to use a Windows computer, a Mac, or a computer running a Linux-based operating system.

The focus on operating systems' capabilities to protect (or infringe) upon your privacy has come into sharp focus recently with certain revelations about Windows 10. Several security and privacy experts found that Windows 10 was an extremely intrusive OS, with numerous privacy-infringing

settings turned on by default.

However, Windows isn't the only operating system that collects usage data -- both macOS and Linux are also culpable of it to some extent, although not as much as Windows. In any case, I hope this chapter has given you an idea of the length and breadth of data that you are currently sharing with the developers of your operating system.

Now, I understand that it is quite difficult to switch operating systems at the drop of a hat. However, I believe that, as a privacy and security expert, I have a moral obligation to inform you of the risks of continuing to use the Windows operating system without-- especially, when it has historically been a large surface area for attacks by adversaries.

Oh, and one other thing: all the telemetry options described in this chapter assume a clean installation of the OS. As you install/add new applications and games to your desktop machine, they may conduct their own telemetry, which may be overt or covert. Spend a little time poking around in the various settings of the application and see if you can spot the telemetry settings.

In the upcoming chapter(s), we'll look at some commonly used applications, the kinds of data they are known to collect, and the different ways to deal with it.

---

[1] This is likely to change soon, since Microsoft has stopped providing support for Windows 7 after January 2020, which was the declared end-of-life date for Windows 7. Organizations may still opt for the extended license, which will provide them with Windows 7 support for another three years, until 2023.

[2] A Unix-like operating system descended from the Berkeley Software Distribution

[3] SPOILER ALERT: This statement is untrue. Macs most definitely do get viruses, albeit fewer than Windows.

[4] MacOS systems have a provision for a ‘super user’ named “root” that is granted all privileges on the system but it is disabled by default. Keep it disabled. Do NOT enable it for any reason whatsoever.

[5] While I do not deny that telemetry does have its uses, I oppose any telemetry that does not provide a mechanism to opt-out. Non-consensual telemetry, in my opinion, is a violation of my right to privacy.

[6] At the time of writing this chapter, this was v1903, popularly referred to as the May 2019 update.

[7] As of the date this chapter was written, the latest available version of Windows 10 is 1903. Windows 10 version 1909 (scheduled for release in November 2019) may be the latest version by the time you are reading this.

[8] Well, the reports are sent to Canonical but that’s one and the same, you know?

Accessing your email

For an attacker, it doesn't really matter at all whether the email is on a server or stored on your local machine, as long as they get some kind of access to it. What truly matters in this scenario is creating enough barriers of entry for attackers to delay them just long enough, so that you can reach out to the authorities.

So, how do you create barriers to entry? By simply following good security practices around your email accessing habits - it's as simple as that, really!

Chapter 8

Desktops-Software Applications

Web-based portals (BASIC, 1 point)

In case you plan on using a browser to access your email through the web-based portal, the standard set of do's and don'ts is applicable.

Always use the secure site - look for https and/or the lock icon in the browser's address bar.

Login to your email only if you trust both the device and the network.

Use your browser's private browsing mode on devices and networks you aren't familiar with.

Log out of your email account and close the browser window when you are done.

Use strong passwords in conjunction with a password manager, wherever possible.

Always use multi-factor authentication to log in.

Understand the terms of service and privacy policy laid out by your email service provider.

In fact, I recommend choosing browsers over smartphone email apps whenever possible, since apps are far more intrusive and have lesser regard for the privacy of your data. If you absolutely must use a smartphone app, choose an app (preferably open-source and trusted) that respects your privacy, such as K-9 Mail, Fair Email, or ProtonMail.

Introduction

While most operating systems these days come equipped with several programs that can read and display all kinds of files, it is virtually impossible to use a desktop without installing any third-party programs.

Take Windows, for instance. Windows comes pre-installed with an internet browser, a music player, an email client, and a bunch of other software that provides the capabilities to read the most common file-types such as ZIPs, TXTs, DOC/DOCXs, PPT/PPTX, and many more. However, most of us rarely use these inbuilt options. It is quite possible that you use Mozilla Firefox (or Google Chrome) as your browser, VLC as your music player, and Mozilla Thunderbird as your email client.

In fact, forget the applications , just answer me this: can you use a Windows machine *without* installing any games on it? Yeah, that's what I thought.

When you install a third-party (read: non-Microsoft) software application on your machine, you increase the probability of exposing some vulnerability on your system. Additionally, if these third-party software applications have the capability to connect to and interact with remote servers, the risk to your privacy is also higher.

In this chapter, we'll look at the concept of third-party software applications that we tend to install on our system and how some of them can have adverse effects on our system and our privacy. We'll also look at the concept of security software which can help mitigate some of these threats.

Offline clients (BASIC, 1 point)

As with web-based portals, I have compiled a list of dos and don'ts for accessing your email through email clients:

Lock your email client with a strong password when you aren't accessing it.

Do not share passwords with your co-workers.

Do not download attachments from unknown senders.

Scan attachments for antivirus and malware after downloading them.

Make regular backups of your email to an external device -- online and/or offline.

I cannot stress how important it is that you do NOT leave either your email client or your system unlocked. Anyone with access to your device or system can easily read through any and every email in your inbox!

Software applications

Before I describe how various software applications can affect your privacy, I'd like to lay down a few definitions:

Authorized software refers to a software application present on your system that has your explicit permission and the proper license required to run it on your system.

Unauthorized software refers to a software application present on your system that does not have your explicit permission OR [1] the proper license required to run on your system.

Essentially, software applications (or programs, as they are commonly referred to) take your input, process it, and provide the output you desire. The word processor, on which this book was written, took the input from my keyboard and mouse and made the last word of this sentence bold . When you visit a website, the browser takes input from your keyboard and mouse and shows you the result in the window, usually in the form of a webpage.

Could you tell me the different points in the process where your personal data could possibly leak in the above examples?

If you said anything close to all points where information is being transported, you would be absolutely right. There are two transport points in the above examples:

Between the input and the processing stage.

Between the processing and output stage.

Of course, if each of the stages has sub-stages, then the transition between those stages is also a potential source of dataleakage. For example, extending the website example, when signing in to a website in a browser window, your password is sent from the browser to the remote server. If this password is not encrypted and someone just happens to be eavesdropping on your internet traffic, your password was just leaked to an unauthorized third-party.

I'm not saying that all programs installed on your system will always leak data or that any and every application you install on your system makes your system immediately vulnerable. However, each new program you add to the system brings with it its own three stages of input, processing, and output, that is, its own points of data leakage.

In fact, the more popular a program, the more likely it is that it will get exploited by malicious actors. Some of the first viruses were transmitted through improperly secured macros in Microsoft Word. There have been several vulnerabilities in Adobe products (Flash, Acrobat, and Reader) over the years that allowed malicious code to be executed remotely on users' systems.

Note

Unauthorized Software andPiracy

Not all software applications directly ask for your password. However, they do have virtually unrestricted access to your system and to most of the files on your system. By allowing them to run on your system, you are essentially declaring that you trust the program not to conduct any malicious activities on your system. By extension, you are saying that you explicitly trust the developer of the program not to include any malicious code that could affect your system, and/or the privacy of your data.

Here's my question to you: can you honestly say that about ALL the programs that you have installed on your system? Even pirated software?

Pirated software is software that has been modified by someone who is not the original developer to force the software to operate outside its licensing conditions. If you are using a pirated software that requires a payment to function otherwise, you are using it in violation of the agreed terms and conditions.

There is another problem with pirated software: whoever modifies the software to bypass any restrictions also has the capability of inserting additional malicious code. Furthermore, the sites that host such pirated content are known to be filled with several advertisements, a lot of which are links to malware. Even the content can be (and often is) severely riddled with malware.

I'm not judging anyone for using pirated stuff -- that's a different discussion, for a different book, for a different day. For all I know, you might even have downloaded THIS book as a pirated PDF or EPUB!

All I'm saying is while piracy may help you save some money, the eventual cost of piracy can be extremely high, so, just be careful!

Compromising your email

Whether you prefer downloading emails to your client or viewing them on web-based portals in a browser, there is a set of basic rules -- a set of Dos and Don'ts, really -- that is applicable to both methods.

Bloatware

Chances are, you might have come across an antivirus, or a game, or a backup utility, or a manufacturer-branded Control Centre installed on a brand-new PC. Some manufacturers will even install full versions of third-party utilities on a brand-new PC. While these programs and utilities are not really essential for the operating system, they, sometimes, do provide additional functionality to users.

These days, operating systems usually ship with a bunch of additional programs and utilities. Especially, with recent versions of Windows (starting with Windows 8 and up), Microsoft began bundling multiple apps such as Bing News, Bing Maps, and many more, along with its standard installation of Windows. On top of that, manufacturers often add their own tools and utilities, with assorted third-party tools and utilities further adding to the clutter in your OS.

Thus, even before you boot your desktop PC or laptop for the first time, you are already saddled with a ton of apps, utilities, tools, and programs that you are unlikely to ever use in your life. Not only do they add to the clutter and consume resources, but some of them may end up actively harming your system and sharing your data with thirdparties without your explicit consent.

For example, in Jun 2019, a flaw was discovered in Dell Support Assist, the troubleshooting software that comes pre-installed with most Dell PCs and laptops. This flaw was so severe that it could allow malicious users to gain complete control of a vulnerable device. Since most users don't pay much attention to (read: upgrade) such as pre-installed bloatware, it was very likely that a significant number of Dell PCs and laptops may still be

affected.

For purposes of this guide, I define bloatware as all programs (third-party or otherwise) that are inessential to the core OS but are bundled with the default installation anyway.

Bloatware on desktops can be typically classified under one of three categories:

Manufacturer-branded utilities

Third-party apps and games

Integrated bloatware

Let's take a look at each one of them and delve into greater detail.

Phishing

Most email service providers do a good job of scanning for such threats and keeping them from even appearing in your inbox. However, as I described in the corresponding section above, ONE email is all it takes to undo all that hard work.

Furthermore, privacy works on the principle of healthy skepticism, that is, even if you trust something, you always look for additional verification. Even if you trust that the email was sent by your friend john.smith@gmail.com , always verify that the email indeed came from john.smith@gmail.com and not john.smith@gmai1.com [1] or some variation thereof.

Moreover, if the email sounds like something John wouldn't usually write, you should always independently [2] verify whether the email was actually sent by john. smith@gmail.com or if his inbox was compromised (that is, Phished) by an attacker. If the latter turns out to be true, the first thing you must do is change the password to your email account. The second thing, help john.smith@gmail.com to change their passwords and send out an email to all contacts in the address book informing of the phishing attempt.

Manufacturer-branded utilities

If you bought your Windows PC from a manufacturer like Dell, HP, or someone similar, chances are you'll find some manufacturer-branded software on your systems. For example, Dell laptops ship with a utility called Dell Support Assist, which allows you to connect with Dell Support when you run into issues with your PC.

Typically, most PCs and laptops ship with manufacturer-branded utility software in order to help maintain your PC. However, this utility only serves a purpose as long as you are registered with Dell Support and within warranty. Once your warranty expires, you are required to purchase an additional warranty to get official support from Dell. Moreover, these utilities are configured to send back various kinds (and amounts) of data about your system to the manufacturer's servers. This is done, ostensibly, to maintain a record about your system and registration with the manufacturer.

In other words, a manufacturer-branded utility serves its purpose for only a limited amount of time and can result in additional expenses and additional data-leakage for the rest of the time.

Here's the thing, though. Almost all the major versions of Windows (Windows 10, 8.1, 8, 7, and even XP) come with similar, in-built utilities that help you maintain your PC. A quick search on the internet will provide you with a solution for your issue that makes use of these in-built utilities instead of manufacturer-branded ones, in almost all scenarios. Depending on your knowledge and technical expertise, it might be either easy or messy to deal with but (in a majority of cases) it won't require you using the manufacturer-branded utility.

Manufacturer-branded utilities may insist that they serve a purpose for the average users of the world. If you were an average user, we'd probably be okay with you letting these utilities exist on your system. However, as a reader of this book, you have clearly indicated that you'd like to improve the security and privacy of your data. I therefore strongly recommend uninstalling these utilities from your Windows PC and laptops.

BASIC: (1 point)

In simple words:

Always verify BOTH the email and the sender!

The most powerful weapons against attempts to gain unauthorized access into your digital properties -- be it email, social networks, online banking, and more. -- are a keen sense of caution and trust your instincts. If you feel something is wrong, then the chances are high that something probably is wrong.

Third-party apps and utilities

Some manufacturers and vendors will include additional applications and/or utilities as a part of the package for the desktop or laptop when you purchase it. For instance, they may include a trial version of a popular antivirus, or a cloud backup service such as Dropbox, or photo-editing software.

With recent versions of Windows, Microsoft has been including various popular apps such as Netflix, Facebook, LinkedIn, Dropbox, and sometimes Suggested Apps such as Candy Crush, and enhanced versions of Solitaire and Minesweeper.

Note

The decision to display Suggested Apps that has been implemented in Windows 10 is devious and distasteful, in my personal opinion. Some of these Suggested Apps appear as a tile in your Start menu, but they aren't actually installed by default. When you click on the tile, you are taken to the Microsoft Store page where you are prompted to install the app on your machine.

Technically, the app isn't installed by default; the installation always happens *with* your consent. However, the fact that it appears on a tile in your Start menu leads you to believe that the app is already on your machine, thus making the whole thing a shade greyer than a 'false' advertisement.

Like I mentioned earlier, you might actually find some (or even all) of these utilities useful. Therefore, it is important that you make a note of all such applications and utilities on your system and figure out for yourself, which of these utilities you absolutely need and which ones you could do without.

In some cases, some of these utilities may not be as benign as they look. Some vendors have been known to ship systems riddled with various kinds of adware, spyware, and other malware -- either on purpose or by accident. I don't have to tell you that adware is not only irritating but it also often ends up slowing down your system. In some severe cases, it can even end up sharing some (or all) of your confidential data with third-parties.

Thankfully, most of these can be easily uninstalled -- I'll tell you exactly how to do it in the #RohitRecommends section further ahead.

Passwords and authentication

No matter how secure your passwords look or feel , there is a possibility that you may not be able to remember them. Moreover, there is a limit to the number of email-password combinations that one can remember.

Based on the details discussed so far, here are my recommendations for managing your login credentials and processes.

Integrated Bloatware

In some cases, the manufacturer-branded utilities might be so tightly integrated with the operating system itself that the uninstall option might not be available at all. This is typically seen with some default Microsoft applications like the Edge browser, or the Groove Music app in Windows 10 installations, or with some manufacturer-branded software on Windows installations.

Unfortunately, not all manufacturer-branded software is designed to be perfectly secure. If a malicious actor were to compromise them, it could result in severe consequences for you as a user, as was evidenced with the Lenovo-Superfish fiasco between 2014 and 2016.

Info

The Lenovo-Superfish Debacle

In 2014, Lenovo announced that its notebooks would come installed with Superfish, a technology that would help users find product offers by analyzing and matching product images while you were surfing the internet.

In other words, Lenovo had installed a piece of software that could intercept your encrypted communication and directly inject ads, based on what you were browsing.

Not only was this a gross violation of privacy, but if this technology were to be compromised by malicious actors, it would serve as an easy way for them to intercept any and all encrypted communications.

What's worse is that Lenovo initially tried to downplay the severity of this behavior by claiming that they weren't monitoring user behavior or recording any profiling information. However, all that changed when researchers from Errata Security presented a proof-of-concept to intercept communications using Superfish software maliciously. In case you are curious, the Errata Security researchers cracked the encryption on the certificate that was at the centre of this mess. You can read the details of how they did it over at their blog by scanning the QR code given alongside this paragraph.

After getting significant backlash from the security community, Lenovo was forced to declare Superfish as vulnerability and provide its customers with removal instructions.

[QR Code: https://blog.erratasec.com/2015/02/extracting-superfish-certificate.html]

Such integrated bloatware can be difficult to uninstall, but it is certainly not impossible. It definitely requires a certain degree of alertness and cares that I have detailed in the #RohitRecommendations section below.

BASIC: (1 point)

There are two different ways you can prevent attackers from easily gaining access to your account. You can use either one or both of these methods to enhance the security of your account.

Use Multi-Factor Authentication: I've already spoken about multi-factor authentication and using authenticator apps like Google Authenticator, Authy, Microsoft Authenticator, and more in a previous chapter but, to reiterate, here's how Wikipedia defines it:

“Multi-factor authentication (MFA) is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism…”

Almost all of the popular websites on the internet -- email services included -- provide multi-factor authentication mechanisms for their users. However, this is not turned on by default; you need to activate this in your account settings. To activate it, you need to either download a compatible authenticator app or provide a phone number that can receive one-time passwords via text message. You will also be presented with a list of recovery codes (that is, codes you can use in case you lose access to your Authenticator app) that you need to store safely.

Regardless of whether you access email through a web-based portal or through an email client, I strongly recommend turning on multi-factor authentication for your email account. The added layer of security is well worth the extra hassle of entering an additional code while logging in to your account.

Password Management Software: Even if you have Multi-Factor Authentication enabled on your email account, you should change/update your password regularly. This is actually easier if you use any of the various excellent password manager services available on the web. Some of the most popular password managers that you can consider using are LastPass, 1Password, Bitwarden, Dashlane, KeePass, and more.

The most powerful argument in favor of using a password manager is the fact that you can literally set a password as long and as complex as N#ifR^T&*YGbnHY!iuGHboi$o!8nC$r9% and never need to remember it! In fact, most password managers come with secure password generators, i.e. automated tools that create random combinations of letters, numbers, and special characters of the desired length, which can be used as an extremely secure password.

Most importantly, NEVER EVER WRITE YOUR PASSWORD DOWN ANYWHERE!

Security software

Given how common internet usage is these days, all desktop devices need a proper security system installed on them to ensure that your personal data stays on the PC. This typically involves installing and setting up a firewall and antivirus software on your machine, more so if your machine is Windows-based.

Of late, due to the rapid increase in malware attacks, installing anti-malware software makes more sense than installing an antivirus. In fact, most antivirus programs also provide malware detection and removal capabilities by bundling all features under one single security suite of sorts.

Let's take a look at each one of these software applications and what they actually do.

Malware

One of the most common methods of malware infection is through malicious attachments sent via email. Malicious actors will typically use one of two approaches:

The Spray-And-Pray Approach: In this approach, attackers send malicious attachments in generic emails designed to evoke curiosity in people. Users unknowingly download the file and try to open it, which results in their devices getting infected with malware.

The Targeted Approach: This approach is typically used by active adversaries, who will send specially crafted emails to increase the chances that the attachment is downloaded and executed.

In both approaches, the ultimate goal remains the same -- infecting the target system with malware that can wreak havoc in the various ways described in the previous chapters.

Based on these scenarios, here are my recommendations for preventing (or mitigating) malware infections on your device.

Firewalls

A firewall is simply an application that looks at every port and monitors the packets of information that is sent or received by each one of these ports on your system.

BASIC: (1 point)

The simplest way to defeat the malware menace and ensure that your device doesn't get infected is to always scan any and all attachments before downloading and opening them. Most popular email service providers (such as Gmail, Outlook, and many more.) provide cloud-based antivirus services, for example, VirusTotal for Gmail.

Info

VirusTotal and Your Email Attachments

VirusTotal was originally created by Spanish cybersecurity company Hispasec Sistemas, launched in 2004, and subsequently acquired by Google in 2012.

It provides several methods to scan your files, including desktop and mobile apps, browser extensions, and API scripts. Scan the QR code given alongside the paragraph to open the Tools section of the VirusTotal website, which lists the various tools available to scan files and URLs.

Antivirus and anti-malware

An antivirus software (or AV software) is a program that can scan, detect and prevent the proliferation of viruses on your system. Viruses are programs that replicate themselves by modifying other programs and inserting their own code, much like their biological equivalents.

These days, however, due to the increased threat of different kinds of malware (such as adware, ransomware, botnets, and many more) most AV software also provides anti-malware capabilities, so it makes sense to club both of them together. If anything, viruses are now considered a subset of malware, but the language used to refer to them is often used interchangeably by most AV developers.

[QR code: https://support.virustotal.com/hc/en-us/categories/360000162898-Tools]

RohitRecommends

Regardless of whether a program is authorized or unauthorized, malicious actors will often try and exploit known and unknown vulnerabilities in the most commonly used programs to try and gain access to a system. Most software developers will issue updates to their programs to patch these vulnerabilities, but it is your responsibility as a user to ensure that you keep your software updated.

So, is updating programs enough to keep malware at bay? How do you protect your data from being leaked? How do you ensure the security of your system and your data? Is not using pirated software enough to avoid being infected by malware?

The short answer is: There is no singular approach that just works .

There are several steps that you must take to ensure that your data remains secure on your system. I'll try and outline them as best as I can but, keep in mind because security is a continuous process, this list will never be 'final' in any way, shape or form.

INTERMEDIATE: (2 points)

If your email service provider does not scan attachments for malware, you can either:

Scan the attachment using a web-based virus scanner , such as VirusTotal.

Scan the downloaded attachment using the antivirus software on your device .

You might also want to consider switching to an email service provider who can (and does) provide better security for your email inbox.

Software applications

ADVANCED: (3 points)

If you absolutely must open a file from an unknown sender, use a good sandboxing software (described in the previous chapter) or a virtual machine to test run files from unknown sources. Malicious files typically [3] can't escape the isolated environment of a sandbox (or a virtual machine) thereby ensuring that your primary system remains unaffected.

Only when you are absolutely sure of the files true nature and intentions, should you open it on your primary system.

BASIC (1 point)

It only takes a single vulnerability in a program to expose your data and render it vulnerable to unauthorized access. That said here are some basic rules [2] that you must set for yourself to ensure the bare minimum privacy of your personal data.

I can't begin to tell you how many times I have been invited to conduct security workshops in offices and found login credentials written on post-its and/or pinned to a softboard in the cubicle. DON'T. DO. THIS.

Always work under the assumption that someone else can ALSO see the text that you are typing into your computer.

If something seems too good to be true , it probably is. That means you haven't won the Coca-Cola lottery and you aren't the one-millionth visitor to a website. No, you won't be able to buy an iPhone by bidding the lowest. The government isn't giving free money, and the Nigerian guy is definitely scamming you.

If a webpage looks suspicious , close it immediately. By suspicious I mean, if a webpage has more than one download button, or wants you to 'complete a survey', or 'hit the monkey', or do some similarly stupid thing to download a file, close it immediately. If a webpage tells you your browser doesn't have a plugin [3] , ignore it and close it immediately.

Update all your programs and update them regularly. You can protect yourself against known vulnerabilities that have been patched by the developers of the software.

Make sure you have adequate security software viz. firewall and antivirus/anti-malware installed and active on your system, and ensure that it is up-to-date with the latest patches and definitions. We'll be discussing these in detail a little later in this chapter.

Encrypt your personal files, especially the ones that have your personal and/or financial information in them. Also, lock your screen before you leave your chair. Log out or shut down your machine if you are leaving for an extended period of time.

Avoid using unauthorized (that is, pirated) software, if possible.

Vulnerabilities are basically 'holes' in the software that can be exploited by attackers to access data on the system without your consent. Patching all the holes properly and quickly is necessary to prevent attackers from exploiting them.

Email ads

Based on the various factors discussed in the corresponding section above, here are my recommendations for countering the privacy-threat posed by email advertising:

INTERMEDIATE (2 points)

Before installing a program, ask yourself the question. Is the developer of this program (individual or company) trustworthy?

While installing a program, pay close attention to the descriptions in the installer window, especially when the installer asks you to make a choice. Programs downloaded from unofficial sites will often include a checkbox to install a secondary product, for example, a free antivirus which is actually malware disguised as antivirus. If any of the descriptions sound confusing, exit the installation immediately and consult with someone who can guide you through the process.

Monitor your security software (that is, your firewall and your antivirus/anti-malware) regularly for any and all kind of suspicious activity. If you spot a program sending a lot of data, consult with an expert as soon as you can.

Most programs will display a notification when something needs updating. However, if you are the kind of person who keeps hitting the Remind Me Later button every time, consider using something like Ninite (https://ninite.com) to automate the installation (and subsequent update) process for your 3rd party programs.

Alternatively, you might want to consider using AppGet (https://appget.net/), Patch My PC Updater (https://patchmypc.com/home-updater-overview) or Npackd (https://npackd.appspot.com/) These are slightly different from Ninite but essentially serve the same purpose.

Change all your passwords on a regular basis, say every three months and, wherever possible, enable 2FA (Two-Factor Authentication) to ensure better security of the data on your system.

BASIC: (1 point)

Understand what data exists within the mails in your email inbox.

Backup and delete any emails that may contain highly sensitive information such as login credentials, passwords, financial information, and many more.

Also, delete unimportant emails from your inbox. Keep your inbox clean and free of clutter.

ADVANCED (3 points)

It is difficult to keep programs from accessing the various parts of your hard-disk once installed. Programs executed with administrative-level access can read (almost) everything on your hard-disk. Thankfully, there are a few ways to prevent your personal data from getting leaked in this manner.

INTERMEDIATE: (2 points)

Migrate your family to a paid plan on your existing email service provider to ensure that your emails continue to stay private and free from any prying eyes.

Alternatively, opt for a free (or paid) plan with a privacy-aware email service (such as ProtonMail, Hushmail, Fastmail, and many more.) that provides end-to-end encryption for your emails.

Sandboxing

If we imagine your system to be your house, then programs are the guests that you invite to your house. Now, if a guest seems shady , wouldn't it be nice if you could hide certain parts and elements of the house from such a guest? Or construct a virtual house of sorts for the guests to visit before you invite them to your actual house?

Well, that's what sandboxing does. A sandbox is an area of your system that is isolated from the rest of your system. Programs installed in a sandbox are allowed to access only the resources available to the sandbox. Therefore, it makes sense to install any new programs within a sandbox to test them out before installing them on your system.

Sandboxing can be accomplished in a couple of ways:

Using a virtual machine: A VM is an operating system installed within an operating system. The guest OS uses the same resources as the host, but all processes and operations on the guest OS are completely isolated from the host.

Using a sandboxing software: A sandboxing software is akin to a virtual machine in the sense that it creates a mini-VM of sorts. However, sandboxing software usually restricts itself to isolating applications and processes, rather than providing an entirely alternative system experience. The most popular sandboxing applications are Sandboxie or Shade.

Sandboxed applications may feel slower than un-sandboxed applications because the programs and processes are filtered through an additional layer of security. However, my opinion is that any difference in speed or performance is definitely worth the additional security that sandboxing programs provide.

ADVANCED: (3 points)

If you own your own domain, chances are your domain service provider already provides you with a (fairly limited) email service, for a specific number of accounts. Several email service providers allow you to utilize their services for your own domain, for example, emails sent to rohit@privacy.clinic can be read using ProtonMail's email service

Consider using PGP extensively in all your email communications, using reliable external, and third-party tools such as GnuPG if, when, and where necessary. You can utilize these tools to encrypt a portion (or all) of your message and digitally sign it with your private key.

File encryption

If sandboxing is akin to hiding your house from shady guests, file-encryption can be called 'locking' your valuables in a safe [4] to prevent 'shady' guests from accessing them freely. Specifically, if you can't (or prefer not to) restrict programs from accessing your data, you might want to

consider restricting your data from being accessed by programs by using good file-encryption software.

There are several files, folder, and even disk encryption programs that are available for various operating systems, ranging from completely free and open-source (FOSS) to completely proprietary and premium. Most operating systems these days even provide (admittedly somewhat limited) file encryption capabilities out of the box. The table is given below lists some well-known file encryption programs that you might want to consider installing on your desktop:

EXPERT: (5 points)

Set up your own email server with end-to-end encryption. There are several tutorials available on the web (and on the companion website privacy.clinic) that will assist you in the process of setting up your own mail-server, complete with open-source spam-filter software.

Be aware that setting up your own private email server requires substantial expertise, not to mention putting in several hours of work to ensure that everything runs smoothly, with minimum fuss. Furthermore, it can be only made as secure as the technologies of the current day will allow it. That means you need to ensure that your mailserver (and the software running on it) is constantly monitored, and kept updated with the latest versions and/or patches.

Spam

The problem of spam is a bit tricky.

On the one hand, as a business owner, being able to send unsolicited commercial communication is definitely a useful tool to have when you are looking to attract new customers. On the other hand, unsolicited commercial communication (specifically the unsolicited part) could be deemed a significant violation of the enduser's privacy.

As an end-user, however, the classification is absolutely clear: Spam is always unwanted, unwelcome, and the less we get to see of it, the better.

To that end, here are my recommendations for tackling spam emails for your email account.

	Win	MacOS	Linux	License	Pricing Model
FileVault	×	(inbuilt)	×	Proprietary	Free
BitLocker	(inbuilt[5])	×	×	Proprietary	Free[6]
GnuPG	✓	✓	✓	Open Source	Free
VeraCrypt	✓	✓	✓	Open Source	Free
AxCrypt	✓	×	×	Proprietary	Freemium
Concealer	×	✓	×	Proprietary	Paid
Folder Lock	✓	×	×	Proprietary	Freemium

Table 8.1: A comparison of commonly available encryption software for various operating systems

These are just a few of the several encryption programs available for your system. Not all of these programs perform the same functions. Some encrypt files, some encrypt folders, some encrypt entire disks, and some do two or more of those three things. Before you install any of them, I strongly recommend you read up on what each one of them does and whether it fits your specific requirements.

BASIC: (1 point)

Regularly train your junk filter by diligently marking any spam mail that may have accidentally arrived in your inbox. Conversely, mark any mail that may have accidentally ended up in your Spam folder, as Not Spam to ensure that future legitimate deliveries do not get accidentally categorized as Spam.

If your spam email has an Unsubscribe link or button, use it.

If your spam email seems to be originating from someone you know, try and independently verify with the known party before clicking any link or downloading any attachments from the mail.

System restore

The final option in this set of recommendations is the option to restore your system to a previous state. System restore is the ability to revert the system back to the state, it was at an earlier time; for example, before a certain program was installed. This comes in very handy if you accidentally install a program that somehow messes up your system.

In Windows, open the System Protection tab in System Properties , which can be accessed by either by:

Right-clicking the My Computer icon OR

Clicking System Infoon the left under Related Settings in Settings | System | About

macOS doesn't have an identical equivalent of system restore in Windows. The closest option available is Time Machine that works by making backups of files to an external storage device. Note that Time Machine does not back up your entire OS the way System Restore does. However, you can use Migration Assistant to restore older backups from Time Machine after a reinstall.

Similar to MacOS, Linux doesn't have a System Restore kind of functionality, but there are a few third-party apps (for example,TimeShift, CronoPete, Back In Time, and many more) that can help you by taking snapshots of your system and restoring snapshots as and when needed.

INTERMEDIATE: (2 points)

Use filters to automatically segregate and categorize email you cannot unsubscribe from into separate folders. Some filters will also allow you to delete the mail without opening it if you want. Tread carefully as this might result in loss of valuable information.

If your email service provider allows it, generate a different alias for your email for different purposes. For instance, Gmail allows you to create an alias with the + sign, that is, if you address is john.smith@gmail.com , then john.smith+amazon@gmail.com, john.smith+flipkart@gmail.com , and john.smith+anything@gmail.com are all valid addresses. Also, john.smith@gmail.com & johnsmith@gmail.com both are the same address, as are j.ohn.smi.th@gmail.com . The number of periods in your Gmail addresses doesn't matter -- they all get sent to your inbox.

Specific details on how to generate aliases for other email addresses can be found in the Help section of your email service provider's website. Typically, you can visit the Account Settings page of your email service provider and check if they provide the alias feature for your account.

Bloatware removal

I have observed that people usually don't bother investigating their desktop PCs and laptops for bloatware. Most users work under the assumption that, If it already exists on the machine, then it must be required. As we have already seen in the previous sections, this is not always true and, in some cases, the exact opposite of the actual truth.

Remember the rules of data-sharing, specifically, rule no. 3?

"If the data is encrypted, but not in your control, then it might be secure, but it is not private."

Clearly, in this case, you are better off removing all the bloatware from your desktop OS installation. Here are a few recommended steps to help you get rid of as much bloatware from your system and keep your system as lean as possible.

Windows 10

Typically, most manufacturers provide a recovery method built-in with their customized version of the Windows 10 OS. Dell, for example, has something called SupportAssist OS recovery baked into most of the Windows 10 PCs, tablets and laptops that it sells.

However, if you're looking to remove manufacturer-branded utilities from your system, this is (obviously) counter-intuitive. Instead, you can try one of the following methods.

ADVANCED: (3 points)

Use a disposable email address to sign up for accounts that require your email address. Websites like Mailinator and GuerillaMail are a couple of examples of popular disposable email accounts with public inboxes. The inboxes can be accessed without a password, and the contents of the inbox are wiped clean every 10 minutes or so.

Hint

A disposable email combined with a strong password, multi-factor authentication, and saved in a password manager is (arguably) a pretty good example of a well-secured login mechanism. Any attacker attempting to breach this set up will have first to crack the (invariably long) password, and then figure out the OTP from the authenticator app.

Alternatively, you can use an email forwarding service such as 33mail or boun.cr to create a second identity which will receive all preliminary email and then forward it to your primary email account depending on rules you have defined. Several hosted email solutions also provide the ability to use them as an email forwarding service.

BASIC: (1 point)

Uninstall programs through the Settings or through Control Panel in Windows. Most bloatware is actually legitimate programs installed but without explicit user consent. If you find a program that you don't want, open the Settings app and then click on Apps . In the section titled Apps and Features find the program that you don't want and click on it. Click the button named Uninstall and Windows will remove it from your system.

If you prefer to use the Control Panel instead, look for the icon that says Programs & Features and click (or double-click) to open it. Find the program you wish to uninstall, click on it, and then click on the Uninstall text/button that appears in the header.

EXPERT: (5 points)

If you have hosted your own domain, or if you are using a hosted email service provider, you cancreate a catch-all [4] email address on your mail-server. Catch-all email addresses send all email that does not have a valid recipient to a single master inbox. Thus, if you have a mailserver running on example.com and you give someone the address jane.smith@example.com , which doesn't correspond to a valid account on your server, the mail will get delivered to the default account on example.com

You can use this feature to create specific email addresses to create separate login identities, for example, amazon@example.com or flipkart@example.com . Essentially, having a catch-all email address is like having a disposable email inbox (such as 33mail or boun.cr) but specifically bound to domain name and mail-server.

INTERMEDIATE: (2 points)

If you've been using your PC for a while and have installed programs that you would rather not install all over again, then consider using a persistent uninstaller program such as the ones developed by IOBit, Revo Uninstaller, or such. Scan the QR code given alongside to check out a (somewhat) comprehensive list of various uninstaller programs.

Prevention and mitigation

[QR Code: https://www.lifewire.com/free-uninstaller-programs-2625188]

Remember, you must always make a system restore point before attempting to uninstall any bloatware -- especially if you have a good reason to believe that uninstalling specific bloatware might destabilize your system! If things do not go as expected, you will at least have the option of rolling back to the earlier restore point.

First, you need to identify the bloatware you wish to remove. To do this, open your Settings app and click on Apps . In Windows 7, this feature is called Programs & Features and it can be found in the Control Panel [7] .

Search (or scan through the list, if you're on Windows 7) and make a note of the apps that are irrelevant to your daily usage. Click on the app to select it, and then click Uninstall to remove it from your system.

Alternately, you can use third-party decrapification tools to help you remove unnecessary software from your PC. These decrapification tools look for common bloatware installed on your system and can often be run as portable programs, that is, you can run them off a flash drive, without needing to install them.

Some popular, trusted decrapification tools that you can use are:

The PC Decrapifier

Should I Remove It?

Slim Computer

A quick search on the internet will provide you with the relevant URLs for downloading and installing each one of them.

BASIC: (1 point)

If like me, you too believe in the saying, Prevention is better than cure then here is a set of three simple instructions that you must definitely follow while accessing your email account:

Avoid public Wi-Fi

Who doesn't love free Wi-Fi? All of us have connected at least once to one of the free Wi-Fi hotspots available at airports, railway stations, and hotels, haven't we?

Here's the thing, if you didn't enter a password while connecting to the Wi-Fi, you might be at risk for an Evil Twin attack on your device. After successfully executing an Evil Twin attack, an attacker, can intercept and monitor all communication to and from your device, without being detected.

That means, not only your email but your social networks, your online banking, your web browsing - everything you do while connected to the Evil Twin Wi-Fi can be intercepted using a type of attack called MitM -- Man in the Middle.

Ensuring that you only visit secure websites (that is, ensuring that the lock is visible in the address bar) while on public Wi-Fi can mitigate some (but not all) of the risks associated with the Evil Twin attack.

The best solution, however, is to never connect to any unsecured wireless networks . If, for some reason, you do connect to one, make sure that the device ‘forgets' the network and delete it immediately from the device.

ALWAYS SIGN OUT OF YOUR ACCOUNT!!

Let's face it; no one typically uses strong passwords for their lock screens, do they? Most screen passwords can be figured out with a little bit of knowledge about the user and the password hint provided by the OS. Put those two together with some smart deciphering ability and, more often than not, you get the lock-screen password right.

Note

I could have included this particular piece of advice under one of the other sections, but I feel I can't emphasize this enough. I can't even begin to tell you the number of times I've found logged in accounts when reviewing security practices for my clients. Accounts containing important and confidential company data that, if leaked, could cause the company huge losses.

Seriously, I can't stress this enough. Always, ALWAYS sign out of your email account and close the browser before leaving your desk!

If you primarily access email through web-based portals, I strongly recommend logging out of your account and closing the browser at the end of every browsing session - no exceptions. Leaving your account logged in because I'll need to open it again in a few minutes or I'm only going to be away from my system for a short while is not just a bad security practice; it is an open invitation to adversaries to compromise you.

A locked screen is probably the mildest deterrent to the adversary who is determined to compromise you and/or your data.

ADVANCED (3 points)

One of the easiest ways to ensure minimal bloatware on a new PC is to perform a clean install. This is definitely recommended for all new desktop PCs or laptops that you may have newly purchased from a manufacturer.

A clean install (typically recommended for Windows-based PCs) involves reinstalling your OS from scratch. There are two different clean-install methods:

Windows Recovery: Open Settings| Update & Security and click on the section titled Recovery in the sidebar. Click the Get Started button and choose the option that says Remove Everything . This is akin to factory-resetting your Windows 10 PC, which means all your manufacturer-branded utilities are likely to return, once this process finishes.

Windows 10 installation Media: Download the Windows 10 installation media from the official Microsoft website and run it on the system you wish to install. If you are prompted to Keep personal files and apps or Keep personal files only, or Nothing, choose Nothing .

Make sure you have backed up all your important documents, exported any important data, and saved all important files to at least two different locations that are not on your machine BEFORE you attempt this step. System Restore points will NOT help in this case.

Understand that you WILL lose all your data, all your apps, all your documents -- everything -- if you perform a clean install on your machine.

"Un-uninstallable"applications

If you come across an application that can't be uninstalled, it could mean one of two things:

The application is necessary for core OS functionality and is marked as a system tool

The application is NOT necessary for core OS functionality BUT is marked as a system tool

The following section is meant merely for your information and is not to be treated as a recommendation of any kind. I recommend that you consult with an expert before you proceed along this path.

INTERMEDIATE: (2 points)

Review account activity frequently

Some of the popular email service providers will send an email to your alternate account if they feel like suspicious activity might be happening on your account. These emails may also provide you with immediate options to mitigate the effects of any unauthorized access to your account.

Almost all the major email service providers store detailed access information about your account, that is, they store details about the times, places, browsers, IP addresses, and many more, from where your account has been accessed. This information is usually available for you to review -- usually in the Privacy section of your Account -- under the heading Activity History or Activity Details something similar.

You should review your Activity History regularly to check if your account has been subjected to unauthorized access by checking and comparing the various details under account activity.

A handy list of dos and don'ts

Do not reply to out-of-character emails even if they are sent by friends/acquaintances.

Always verify the name and email address of the sender properly and carefully.

Do not reply to emails sent by random strangers.

Be VERY careful with attachments!

Do not open attachments that make you log in to a website.

Do not use public networks to access any personal or professional email accounts.

Regularly review the Account Activity of your email account.

Never write down your login credentials anywhere.

Encrypt your emails with PGP, whenever and wherever possible.

Bookmark this page for quick access, in case you need a reminder.

EXPERT (5 points)

Modern versions of Windows, (that is, versions of Windows 8 and above) come pre-installed with a bunch of applications that don't serve much purpose other than cluttering up your system and infringing on your privacy. These applications are also marked as system applications which means that they cannot be uninstalled using the method outlined in the previous section.

Fortunately, there exist multiple free, trusted, third-party tools such as O&O App Buster and Windows X App Remover . These tools [8] are aimed at specifically uninstalling such pre-installed Microsoft applications. Furthermore, since these tools are portable, that is, they don't need to be installed, you can download and run them off a flash drive if you so wish.

Important!!

ONCE AGAIN, I DO NOT RECOMMEND DOING THIS WITHOUT PROPER SUPERVISION BY AN EXPERT!!

Be very careful with what you choose to remove and always, ALWAYS make a system restore point before you remove any un-uninstallable applications. If things go south, you can always restore your system to the system restore point and prevent yourself a huge headache.

Also, conduct the necessary research (or, at least a quick search on the internet) to ensure that the software you are trying to uninstall is, indeed, bloatware. Some packages might look suspicious (for example, Microsoft .NET Redistributable packs) but are actually essential because other important programs on your device may be dependent on them.

Conclusion

Your email address is not just a token for communication -- it is a core part of your identity on the internet.

In fact, most of us often use this same email address to sign up for various websites and services on the internet. There is a significant chance that the email you use to log in to Facebook is the same as the one you use for twitter, Snapchat, Instagram, and many more websites. Usually, the

argument for doing this goes along the lines of, Well, I don't have multiple identities in real life, why should I have them online! or I don't have time to remember multiple email and password combinations!

However, by reusing the same email address for all your identities, you are essentially providing both advertisers and adversaries with a complete package of your data under one single identity -- your email address.

What happens if that identity gets compromised? Or worse, what if it entirely ceases to exist? For example, if Google decides to shut down your account, what would happen to all your online identities? What would happen if Google were to shut down the entire Gmail service? They don't *have* to continue providing Gmail as a service, especially as a free service, do they? Would you be able to switch to a different email provider quickly and painlessly?

You have a responsibility to take every effort to ensure that this identity -- this core identity that defines a large part of your existence on the web -- does not get compromised easily.

---

[1] I hope you noticed that the ‘l’ in the email address is actually the number ‘1’.

[2] You could call or send a text, or meet face-to-face, etc. to confirm.

[3] Some advanced malware can used sophisticated techniques to identify sandboxing (or virtual systems) and change its malicious behavior accordingly.

[4] A ‘catch-all’ email address, as the name suggests, is an email address that accepts and receives all incoming email and redirects it to different inboxes depending on the specific identity on the incoming email.

Apple (macOS)

Chapter 11

Software-as-a-Service (SaaS)

BASIC: (1 point)

For Apple devices (that is, devices that run macOS) as their primary operating system, bloatware isn't much of a problem because Apple systems don't ship with much bloatware (except stuff like GarageBand, Movie Maker, and many more, which you may not need) and if you see a program or a utility you don't like, you can simply uninstall it as follows:

Open the Launchpad, that is, the spaceship/rocket-shaped icon in your dock to open a list of currently installed apps.

Find the app you want to remove and click and hold the app icon. An x will appear on the top left of the icon, and the icon will start shaking.

Click the x and click Delete when prompted.

That's it. You're done.

Introduction

Email is no longer the only reason people use the internet.

These days, the internet provides various other utilities that have far surpassed email in terms of usage, both retention-wise and frequency-wise. It is not uncommon to see people opening multiple websites in different tabs in the same browser window. We often log in to our email in one tab, check out what our friends are doing on Facebook, or LinkedIn, or Instagram in another tab, browse products on Amazon, or Flipkart, or Myntra in a third tab, conduct some financial transactions in a fourth tab, and so on.

The internet has given birth to a multitude of services, all aimed at replacing some task or the other -- tasks that would take a significantly greater effort in real life. Through social media, we are able to stay in touch with our family, friends, and acquaintances. Email and instant messengers have completely replaced the traditional postal mail in most scenarios. Not many people visit the bank these days -- most banks provide a netbanking portal for people to carry out a lot of the commonly executed financial transactions. Shopping for something has become a lot easier thanks to multiple e-commerce sites that sell products catering to a wide variety of interests. Even planning holidays has become a lot easier thanks to travelling websites that provide end-to-end services, which you can access by simply logging in on their websites!

These websites that provide specific services over the internet are commonly referred to as SaaS, which stands for Software-as-a-Service. The companies behind these websites design and develop the software but, instead of selling the software as a product that people can purchase and use, they host the software on a central server and provide access to individuals who wish to use the product.

Linux

Linux machines usually don't ship with bloatware. That said, if you happen to come across any non-essential application or software that you don't need on your system, you can use your system's package manager software (either command line or GUI) to uninstall that particular software and its various dependencies.

So, what exactly is SaaS?

SaaS is what people usually mean when they say your data is stored in the 'cloud'. Think of SaaS as just another way to describe a specific service that you are accessing over the internet.

For example, imagine you are a student, searching for answers to a highly specific question. In the earlier days, you'd spend all the time looking in the library rifling through various reference books to find a satisfactory answer. Alternatively, if you were looking on the internet, you'd start by opening a somewhat relevant website and depend on reference links to investigate further.

In fact, this is how early search engines operated. Search engines like Altavista, Ask Jeeves, and Lycos, would read through their index of millions of websites on the internet and pop up results when the search query appeared among them. Searching the internet would sometimes take seconds or even minutes, and it was heavily dependent on whether or not you used the 'correct' search term! Google changed the whole search engine game by adopting a different methodology that returned results in several orders of magnitude quicker. Where searches could sometimes take minutes to execute, Google almost always returned results in milliseconds.

Info

As of August 2019, Google still shows the time taken by its servers to perform the search. You can see it in parentheses next to the number of search results.

Most regular searches are performed in less than a second, but if you can craft a somewhat lengthy, vague-ish query, you can make Google work for a couple of seconds. Go ahead, try it!

Now, Google could package this unique search engine technology into installable software and sell it as a product that everyone could install on their PCs. However, indexing and storing millions of webpages requires massive computing power that is not affordable for everyone. So, Google decided to offer their software , that is, their advanced searching technology, as a service to anyone who desired to use it.

In other words, Google chose to host their software on a central server and offered it to all users across the internet, as a service anyone could use by visiting their webpage.

One might argue that the internet was designed to connect us to various people and services across the world, and exactly that is what SaaS ensures. However, by now it must be obvious to you, dear reader, that each new SaaS that you sign up to is a potential attack vector. In fact, each new tab that is opened, each new website that we sign in to, is another avenue for a potential attack on our privacy and our personal data.

BASIC: (1 point)

For example, suppose you want to uninstall jabber (a messenger application) from your default Ubuntu or Linux Mint install. All you have to do is open the Software Center, search for a package named Jabber and click uninstall. Alternatively, just run the following command:

$ sudo apt-get remove jabber

And enter the root password, and the application will be uninstalled. Simple, isn't it?

Types of SaaS

When you think about it, any websites on the internet that require you to sign up would be classified as a SaaS - email, social networks, netbanking, e-commerce - all of them are software programs that are provided by their developers as a service.

Broadly speaking, all SaaS can be classified into four categories:

Social SaaS

Shopping SaaS

Financial SaaS

Other SaaS

In the sections that follow, we'll be providing a few examples of popular SaaS in each category, what data they expose, how vulnerable they could

be, and some ideas on how to secure any accounts you might have on their servers.

Security software

Regardless of how secure you think your system is, installing good security software is always recommended. At the very least, setting up a good firewall and an antivirus should be considered a bare minimum for every desktop system that you use.

I'll outline a few examples of how to get the best out of your security software and the usage hygiene you need to implement to make that happen. Remember, security is not an end-product -- it is a mentality that you need to cultivate and implement.

Tips

I strongly recommend NOT using any 'unknown' systems, especially if they don't use at least a firewall and an antivirus, e.g. computers at a cyber-café. Chances are, you might end up unknowingly leaking crucial personal data (such as your netbanking credentials) to an eavesdropping malicious actor.

If you absolutely must log in to an unknown system, make sure that you immediately change the credentials from a 'known' computer in order to mitigate any potential damages arising from the act.

Social SaaS

All Social SaaS contribute to one of the largest uses of the internet and can be broadly divided into two categories:

Social networking: Social networking SaaS primarily focus on connecting you to various people and/or businesses that you know and interact with.

Social media: Social media SaaS is designed to collect information from a selection of sources much, much broader than your network and present them to you.

These two capabilities of Social SaaS -- networking and media -- need not necessarily be exclusive. In fact, in some cases, a single SaaS can have both networking and media capabilities embedded in the architecture and design of the SaaS. Facebook, Twitter, Instagram, or LinkedIn are good examples of a combined SaaS.

Other apps may choose to focus on one capability over the other exclusively. For instance, WhatsApp focuses on providing instant messaging between people by connecting them through their existing phone numbers.

The common examples are Facebook, Twitter, Instagram, LinkedIn, WhatsApp, Snapchat, Line, WeChat, Hike, YouTube, Twitch, TikTok, Discord, Reddit, Pinterest, Tumblr, VK, Flickr, Meetup, and many more.

Windows 10

Simply put, due to the massive numbers of attack vectors present in the wild, every Windows 10 system needs to have security software installed and active.

Let's look at the various options for both kinds of security software (firewalls and antivirus/anti-malware programs) that you have at your disposal for your Windows 10 system.

Firewalls

Shopping SaaS

One of the first innovative uses of the internet was the ability to simply log in to an e-commerce website such as Amazon, or eBay and purchase a product you wanted. Over the years, e-commerce has grown from selling just physical products to selling all kinds of products and services - both physical and otherwise. You can buy gifts, hire cars, order food, rent hotels, book vacations -- basically any and all kinds of goods and services at the touch of a button.

In fact, under this category, we include all apps that provide any kind of product OR service in exchange for money. Therefore, along with the standard e-commerce sites like Amazon, Flipkart and eBay, we'll also include cab aggregators, travel and holiday planners, classified ads, delivery services, and many more.

However, this fantastic ability to shop for goods and services online comes at a price - pun unintended.

Every time you buy something on the internet, you are also sharing a bunch of highly private and sensitive details, such as your name, your address, your financial details, and other private details such as the products you are interested in, with the shopping site and its partners. You implicitly trust them to keep all that data secure.

The common examples are Amazon, Flipkart, Myntra, Snapdeal, Ajio, AliExpress, eBay, OLX, Quikr, Swiggy, UberEats, Zomato, UrbanClap, Dunzo, BigBasket, Ola, Uber, Cleartrip, MakeMyTrip, Yatra, and many more.

BASIC: (1 point)

All Windows 10 installations automatically come with an inbuilt security solution named Windows Defender, right out of the box. Windows Defender is a suite consisting of a firewall and an antivirus with malware-detection capabilities.

The Windows Defender Firewall is a part of the Windows Security app which can be accessed through the Start menu, or by opening Settings | Updates & Security | Windows Security and clicking on the button titled Open Windows Security .

Open the Firewall & network protection section from the sidebar and ensure that the firewall is on for all three kinds of networks, that is, Domain Network, Private Network, and Public Network.

If, instead, you see a button named Turn On , click the button to activate it.

Financial SaaS

In my honest opinion, one of the biggest advantages of the internet has been the availability of banking and financial services online. Being able to access account details and conduct transactions over the internet have been a blessing in so many ways, hasn't it?

Gone are the days when you needed to visit your bank branch and stand in the queue to transfer money from one account to another. These days, all you need to do is enter a bunch of numbers on your bank's netbanking portal, and the banking SaaS takes care of the rest. Getting your latest account balance doesn't require you to go to the bank and get your passbook updated -- all you need to do is open your banking app and, voila, there it is!

In fact, banks these days even provide their own smartphone apps that let you access a ton of banking and financial services. You can use your bank's official smartphone app to perform various tasks such as accessing your account details, transferring funds, managing various financial instruments such as FDs, PPF accounts, credit cards, and loans.

To ensure the highest level of security in online and smartphone interactions, banks often go the extra mile, much beyond the standard step of implementing a secure communication layer between your browser and the remote server. Most banks implement some extreme security measures in place on their netbanking portals, for example, disallowing common browser behavior (such as, right-clicking, or hitting the back button or the refresh button) or forcing you to change passwords every six months, or making you re-login after an extended period of inactivity. As a matter of fact, if your bank's portal or smartphone app does not have such extreme measures in place, you might want to reconsider your relationship with the bank!

Note

Even if your bank doesn't require it, it is a good idea to change your netbanking passwords every six months. Privacy experts are equally divided between committing the password to memory and using a password manager, so we'll let you decide for yourself. In any case, do not write your banking credentials where they can be seen or accessed by others.

However, banks aren't the only financial SaaS available over the internet. There exist a category called NBFCs (Non-Banking Financial Companies) that provide independent SaaS-based portals and smartphone apps. These are often hybrid apps that are primarily designed to provide easy payment mechanisms and also integrate corollary shopping experiences to incentivize usage of their SaaS.

The common examples are ICICI, HDFC, SBI, IDBI, Pockets, PayZapp, Yono, PayTM, Google Pay, mPesa, Freecharge, MobiKwik, and may more.

INTERMEDIATE: (2 points)

If for some reason, you do not trust Windows Defender, you also have the option of installing your preferred third-party firewall. There are several free and paid options you can choose from, ranging from popular names such as Comodo, Norton, and ZoneAlarm to lesser-known but superb options such as TinyWall, GlassWire, and PeerBlock.

Other SaaS

This section encompasses all those SaaS that do not neatly slot into one of the above categories but still run in the cloud . Examples under this category might also fit into multiple categories without falling neatly into either one of them.

For instance, StackOverflow and Quora are SaaS websites that operate a Q&A service, but the user interactions and website design indicate a secondary focus on social networking. Similarly, Slack and Discord are primarily collaborative apps, but they have found use as the modern IRC and Yahoo! Chatroom equivalents. Dropbox, Google Drive, and Box provide document storage services -- something that doesn't fall neatly under any of the categories mentioned above.

Essentially, this category encompasses all services that fulfil ALL three criteria:

Run their operations in the cloud that is, on remote servers.

Provide an interface to access these services over the internet.

Do not qualify neatly under any of the above categories.

The common examples are StackOverflow, Office 365, Dropbox, Google G Suite, Box, WebEx, Zoom, Zapier, JiRA Atlassian, Confluence, Slack, Keybase, Discord, GitHub, and many more.

Antivirus & Anti-malware

Privacy and security concerns

I would like to acknowledge here that most popular SaaS websites take security and user privacy very seriously.

However, that doesn't mean they are totally invulnerable. There is no perfectly secure solution that covers all possible adversaries and all kinds of attacks. If it did exist, every website in the world would already be using it. However, it would still leave one aspect of the service vulnerable - the user themselves.

Due to its very nature, all SaaS directly violates the first two guiding principles of privacy:

No local data storage -- retain no information locally about the user and their activities.

No remote data storage -- do not sync user data (encrypted or otherwise) to a remote server.

All the information you share with any SaaS websites is stored on their servers, accessible to you behind a username and password. That means all the thoughts and updates you post, all the messages you send, all the personal details you add to your profile, all your purchases and transactions, all your payees and accounts, are stored on servers controlled and managed by the SaaS.

No matter how secure you make a website, there are quite a few weaknesses of users [1] (such as gullibility, oversight, and many more) that can still be exploited. Therefore, it is extremely important that users are made aware of good security practices so that these attacks are mitigated.

In the sections that follow, I will try and outline as many of these SaaS-related privacy concerns as possible.

BASIC: (1 point)

The Windows Security app also has a section in the sidebar titled Virus & threat protection . Click on it and ensure that the text under the heading Virus & threat protection settings says no action needed. If, instead, you see a button named Turn On, click the button to activate it.

Note

The malware detection service (also referred to as threat-protection in the Windows Security app) can be a little unreliable at times. I recommend installing at least a competent anti-malware program (such as MalwareBytes Anti-Malware or SpyBot Search & Destroy) and using it in conjunction with Windows Defender.

ToS and privacy policy

When you sign up for an account for a particular SaaS, one of the things it requires you to do is agree to the Terms & Conditions and accept the Privacy Policy. Almost all of us click the checkbox without bothering to read anything. Due to legal ramifications, companies will always specify their data-sharing policies in their Terms of Service (ToS) and Privacy Policy documents.

In some cases, some companies might even willingly compromise a user's privacy through data-sharing policies that are harmful to the user's privacy. However, since most users don't bother to educate themselves, these companies often manage to get away with it.

Example

A recent example would be the furore caused by a popular photo-manipulation app known as FaceApp. Users who downloaded the app and signed up were shocked when they realized that, according to the Privacy Policy, they had consented to share their data and giving the company all the rights over any images created by using the app! In other words, all images created using a photo app were automatically licensed by FaceApp for free and in perpetuity!

Sadly, due to the one-way nature of the transaction, there is no way to review and revise the ToS or the privacy policies presented by companies – it is a binary exchange in which you can either agree to the terms presented or refuse to use the service in its entirety.

Some courts have ruled that the ToS is not strictly enforceable if they happen to violate the fundamental rights of users. However, in most cases, the terms of service are usually accepted as a binding agreement between the user and the service provider.

Read the Terms of Service; most companies offer a simple language version of their terms of service, where they outline and explain in simple words the terms on which they provide the service to you. These are usually made available at the bottom of the website, or can be found by using the search function on the SaaS website.

Alternatively, you can use the excellent service named Terms of Service; Didn't Read, (abbreviated to ToS;DR) which classifies the terms of service of several commonly used SaaS on a decreasing scale from class A to class E. The service is available as a website and as a browser extension and can be accessed by scanning the QR code displayed on the rightside of this paragraph.

INTERMEDIATE: (2 points)

Similar to firewalls, if you want something more than the inbuilt Windows Defender, then you can install your preferred third-party antivirus software. In fact, there are tons of third-party antivirus programs available for your Windows 10 system, with both paid and free versions that you can download and install. Among the most popular are BitDefender, Avast, Avira, ESET, Kaspersky, QuickHeal, and many more.

Some of these programs may even provide multiple internet security solutions, that is, they protect against viruses, malware, intrusions, scamming & phishing attempts, and many more, for a fee, that is, paid version.

Note

Simply having a good firewall and antivirus program on your system isn't enough.

Sure, firewalls and intrusion prevention systems can identify and block several threats, but, sometimes, some threats can slip through the cracks. Sometimes, malware can lie dormant until certain conditions are met and then suddenly become active. Scanning your system regularly for infections and threats helps mitigate some of these risks and may help prevent untimely loss of valuable data.

[QR Code: https://tosdr.org/]

macOS and Linux

You'll hear a lot of people claiming that both macOS and Linux are malware-resistant, that is, there is very little chance of them getting infected by a virus or malware.

This is not entirely untrue. Linux and macOS insist on user accounts that do not have administrator (or root) level access. Thus, any applications installed for a user are installed specifically for that user, and the installer is typically not given system-wide permissions. This level of compartmentalization ensures that any malicious programs do not get to infect the whole system. However, they may still act as carriers for viruses, that is, carry potentially malicious executable (a.k.a. EXE files) that might infect other Windows PCs.

Therefore, one of the arguments for running antivirus software on your macOS or Linux system is to ensure that the other Windows systems on your network (if any) do not get infected!

So, let's look at some options for firewalls and antivirus on macOS and Linux systems

Service reliability

For a SaaS to be considered reliable, the two most important things to consider are the security and stability of the software. Software that can be easily breached by external adversaries will not survive in the market. Software that is frequently unavailable will also not survive in the market. However, a SaaS-based application that achieves a significant level of popularity (and thus, reliability) will also suffer from adversarial attacks from actors looking to breach into its data.

Maintaining reliability is, thus, a constant endeavor for any SaaS-based application looking to establish itself in the market. Conversely, a SaaS that cannot ensure reliability will be forced to stop operations and cease service.

What happens to your data if a particular SaaS that you rely on decides to stop operating? Can you port your data to another similar provider? Will either SaaS (the one that is shutting down vs the SaaS that you are looking to move to) provide mechanisms to move the data from one to the

other? Or is it simply enough to provide a way to download all your data?

Example

Recently, Google Plus announced that they would be shutting operations and users were provided instructions to download their personal data using Google's Takeout service. While this was a great option for ardent users of Google Plus, it was mostly an empty solution because the downloaded data could not be re-uploaded to any of the other SaaS available in the market.

Another similar example was when the popular Google Reader decided to cease operations. In that case, however, other similar SaaS applications such as Feedly, and more, stepped up to provide an easy way to import people's existing Google Reader subscription lists to their accounts.

BASIC: (1 point)

Firewalls

macOScomes with an inbuilt firewall which is turned off by default. To enable this, open the Launchpad and click on System Preferences . In the Firewall tab, select the grey radio button titled Firewall: Off to turn on the firewall. The change will be signified by the grey radio button turning green.

According to the website AverageLinuxUser.com, you do not need [a firewall], but it is better to have [one]. The most commonly used Linux systems (for example, Ubuntu) have a firewall included in the kernel, which can be configured using the iptables package, but the interface is disabled by default. You can install gufw (short for Graphical UFW or Graphical Uncomplicated Firewall) to configure rulesets as per your requirements.

Security and transparency

Imagine being told that a particular lock is the best and the strongest until it hits the market and someone managed to break it on the first day using just a simple, cheap screwdriver! How embarrassing, isn't it?

In this scenario, the lock manufacturer relied on the most common principle of security, which is security-through-obscurity. By not revealing the kind of security implemented, the manufacturer hoped to dissuade adversaries from breaking into the lock. However, all applications of security-through-obscurity are almost always subjected to brute-force attacks -- in this case, the screwdriver.

A better approach to security, rather surprisingly, would have been the security-through-transparency approach.

Think about it: if the lock had been subjected to rigorous tests and audits by a competent external third-party, there is a good chance that someone would have found that the lock was vulnerable to brute-force screwdriver attacks much earlier!

Similarly, a competent SaaS-based application or website will ensure maximum security of any and all user data by allowing it to be thoroughly tested and audited by both internal stakeholders as well as external experts. Examples of this behavior can be seen with a lot of popular social networking websites and applications such as Facebook, Instagram, WhatsApp, GitHub, and many more. All of them offer bug-bounty and responsible disclosure programs for external security researchers, a.k.a. ethical hackers.

Getting these ethical hackers to communicate such exploits to the developers and maintainers of the software first allows the developers of the software to fix it before malicious actors are able to take advantage of it.

As I have said constantly, security is not an end goal to be achieved; it is a state of awareness that needs to be constantly reinforced. True security is when you can successfully adapt to any threatening circumstances that may develop with the passage of time.

[QR Code: https://averagelinuxuser.com/linux-firewall/]

Security breaches and response

Regardless of whether your SaaS chooses security-through-obscurity or security-through-transparency, your SaaS must have a standardized protocol to respond to security breaches.

Thankfully, more and more regulators across the world are stepping up and making it mandatory to inform users within a reasonable timeframe as a matter of legal compliance.

For instance, the RBI fined Yes Bank to the tune of USD 1 million for failing to notify its users of a 2016 breach that put 32 lakh debit cards at risk. Europe's GDPR (General Data Protection Regulation) laws that went into effect on May 2018 requires companies to notify regulators of breaches within 72 hours, under threat of a maximum fine of 2% of worldwide revenue.

No SaaS is so perfect as to stay successfully unbreached forever. However, a good, competent SaaS will have a properly documented response plan in place with instructions on how to triage and contain the situation, assess the severity and damage, notify the affected users, and educate them on how to prevent this from happening in the future.

Example

Recently, in March 2018, a bug was found in Google Plus by the developers of the SaaS and (according to them) was immediately patched. The discovery and patch were both left undisclosed by the developers who claimed that no data was leaked according to their investigation.

The incident would have gone completely unnoticed were it not for the Wall Street Journal who revealed it in October 2018 -- a full seven months after the incident.

Antivirus and anti-malware

macOSdoes not have antivirus software built into it, be the default. macOSdoes have a feature called GateKeeper. GateKeeper is a service/feature that prevents you from installing apps that are not from the Mac App Store and/or from identified developers. macOS also has File Quarantine, built-in anti-Malware protection, which is very similar to the SmartScreen feature deployed by Windows. It checks downloaded files against known malware definition signatures and warns you if a match is found. However, compared to Windows Defender, both these alternatives are fairly rudimentary.

Linux systems do not have any antivirus software installed by default or built into the system because they genuinely do not need it. However, there are several third-party applications that you can download and install, details of which I'll provide in the next section.

Security updates

There have been occasions where vulnerabilities were found at system-level or hardware-level that affected a wide variety of devices and services and not just a specific SaaS. In situations such as these, it is extremely important to ensure that the SaaS provider updates to the latest patch in a quick and timely fashion.

For instance, the vulnerability nick-named Heartbleed was a serious vulnerability in the OpenSSL cryptography library that could compromise secret keys generated by this library and allow attackers to eavesdrop on encrypted communications. It was introduced into the software on 14th March 2012, but it was only made public on 7th April 2014, with the patch being released on the same day.

Note

The OpenSSL library is used by webservers such as Apache and nginx, which constitute about 66% of all active sites on the internet, that is, 66% of all active sites on the internet were immediately vulnerable to this bug.

Furthermore, email, servers, VPNs, and a wide variety of desktop software that used the vulnerable version of OpenSSL was also affected.

In the aftermath of the revelation of this vulnerability, it was urgent that all applications (SaaS-based and otherwise) were patched with the update to prevent further damage. Companies and individuals across the world scrambled to patch their systems. However, there is a fair chance that some systems may have been left unpatched due to ignorance, inertia, or (worse) plain incompetence.

If your SaaS provider falls into the category of people who did not patch their systems, where does that leave you and your data? It also raises the question: should you continue to have an account with said SaaS provider?

ADVANCED (3 points)

There are several third-party alternative firewalls, antivirus, and anti-malware software, offering several additional features that you can install on your macOS and Linux systems. Note that the list provided below was constructed in September 2019 and it may have significantly changed since then.

You can always find an updated list at the companion website for this book, that is, https://privacy.clinic . Simply scan the QR code given alongside this paragraph to open the home page on Privacy Clinic in your phone browser, right now.

[QR Code: https://privacy.clinic/]

Firewalls

While the default macOS firewall does a pretty good job of monitoring your internet traffic, those of you who wish for something more detailed might want to consider installing one of the following on your macOS system:

"Hands Off!" by One Periodic

"Little Snitch"

Murus

Radio Silence

Avast Internet Security

Most of these firewalls are available in both free AND premium versions. The free versions usually offer just the basic firewall functionality with a better interface than the inbuilt firewall but, in most cases, the premium versions (typically) offer slightly enhanced features. Some providers such as Avast may even provide the firewall, antivirus and anti-malware features combined in one single package.

Also, please note that this list is not exhaustive -- there are several other options that you might want to consider. For the latest recommendations, check out the QR code given at the beginning of this section.

Data access

Typically, users of a SaaS-based application or website may choose to access their data in one of two ways: online or offline.

Allowing a SaaS to be accessed online is definitely a huge convenience -- since it can be accessed from virtually anywhere on the planet. However, that is also what makes it significantly more insecure. For instance, what happens if you log into a SaaS account, for example, a shopping site like Amazon, on a browser in a library or a cyber-café and forget to logout?

Antivirus and anti-malware

sidered to be marginally more secure. However, since it stores your SaaS data on your local machine, the data is only as secure as you can make it.

Similar to firewalls, there are several free (and premium) antivirus & anti-malware software programs that can be downloaded for macOS. Most of the well-known antivirus companies offer both free and premium antivirus solutions for both macOS and Linux-based systems. Some options you might want to consider for your macOS system are:

In either case, the SaaS needs to ensure that the data being displayed to the user is:

Securely stored

rity

Securely transported

Intego Mac Internet Security X9

Within all applicable legal framework

Sophos Home

The last point is particularly important because of the complications that arise when data crosses borders - which it inevitably does when it travels over the internet. For example, Switzerland, a country that guarantees the right to privacy in its constitution, has made it mandatory by law for SaaS providers to store all of their data within the borders of Switzerland.

Malwarebytes Anti-malware

A SaaS that does not ensure secure storage and transport of data and does not respect the legal framework will end up losing the trust of one or more of its three stakeholders -- the consumer, the investors, or the government.

Among others, whereas for Linux-based systems, you might want to consider installing one of the below options:

Clam AV

Comodo Antivirus

Sophos Antivirus

ClamTK

Chkrootkit

Example

Rootkit Hunter

An example of this is watching movies on Netflix.

As mentioned earlier, a list of the current most popular options will always be made available at privacy.clinic, the companion website to this book. Scan the QR code given alongside this paragraph to view the companion website in your browser.

The movies are intellectual property that Netflix temporarily licenses, and it needs to (reasonably) ensure that the movies cannot be copied without permission -- either from their servers or while being streamed to the user. Moreover, since the licenses acquired by Netflix are geographically-specific, Netflix needs to ensure that content licensed for India does not get streamed to subscribers who do not have a Netflix India subscription.

[QR Code: https://privacy.clinic/]

RohitRecommends

In recent times, several regulatory bodies have developed frameworks to streng then the privacy rights of internet users, especially users who sign up with various SaaS providers. These frameworks serve as an excellent guideline for checking and tuning privacy settings as well.

Therefore, keeping in mind the privacy concerns I noted above, there are a bunch of actions that I would strongly recommend for SaaS users. Each of these actions requires you to sign into a specific SaaS provider and locate the corresponding setting to execute the recommended action.

In other words, we'll be using generic terms (such as My Profile) to describe the setting, but each SaaS provider may use slightly different terminology (such as Account Details or Profile Details) for the same. I advise you to spend some time carefully working through this checklist to ensure optimum privacy (or maximum privacy) for your profile data stored with the SaaS provider.

As you read through the following sections, you will also note that I am not providing specific actions to take for mitigating privacy threats on these SaaS websites. This is primarily because the actions will differ from person-to-person and also because it will also differ depending on individual circumstances.

For instance, a person looking to be forgotten by the internet might want to either delete or randomize/anonymize their information. However, for most people, it probably makes sense to keep these personal details filled in -- especially on shopping and financial SaaS websites -- to save themselves a bit of time and typing during future logins.

Conclusion

Without a doubt, Windows is the target of choice for malicious actors and hackers looking to access data in all kinds of unauthorized manner. However, that shouldn't be taken to mean that macOS is the safer option, though. With the popularity of Apple devices increasing every day, macOS and iOS will soon become a viable target for malicious actors to develop potentially harmful malware.

Already, according to the 2018-19 security report from AV-TEST [PDF], the number of malware programs for macOS has almost tripled […] there were nearly 100,000 samples found that affect Macs in 2018.

Types of SaaS

Ideally, in this section, I should be providing you with specific steps, techniques, and/or tools to tweak the various privacy settings with all the SaaS websites that you might have signed upon. However, there are so many of them that it obviously makes no sense for me to go into explicit detail for each SaaS website specifically.

Thankfully, most SaaS websites follow a similar pattern for designing their account settings, that is, the section of the website that allows the end-user to make the changes that impact the privacy of their data and security of their account.

Therefore, my recommendations will be designed to give you a broad idea of where to look and what to look for, so that you can conduct your own investigations, draw your own conclusions, and execute them in a way that ensures optimum privacy of your personal data.

The best way to get maximum utility for this chapter would be to follow all the recommendations given in this chapter for each one of your SaaS accounts.

IMPORTANT: Scoring Instructions for this section…

In the section above, where I detailed the different types of SaaS, I have provided common examples of various SaaS websites which fall in that list. Read through the common examples in each category and make a detailed list of all the SaaS that you may have signed up for.

Alternatively, search your email inbox for words such as registration, account details, or similar and then make a list of all the websites that have sent you registration emails. Usually, these websites send emails from a no-reply address, so using that as a search term might yield a few results, as well.

Info

Once you have the list, here's what you'll need to do:

Identify and categorize all your SaaS accounts into one of the following four categories: social, shopping, financial, and other.

Go through your list one-by-one and open the Settings and/or Profile page for that specific SaaS account.

Follow the recommendations given below for each one of your SaaS accounts, as per your needs and requirements.

Keep a running tally of the points earned for each of the SaaS websites – you'll need it to calculate your final score for this section.

Regardless of how many sites you have signed up for, award yourself the average of the points tallied (rounded down, not up) for the recommendations followed for all the sites in your list. For example, if you deleted your Facebook account, made your Instagram account private, and anonymized your Twitter, Reddit, and StackOverflow accounts, that earns you 5+2+3+3+3, that is, 16 points.

Averaged over 5 SaaS websites, that's just over 3 points per site, which is how much you should award yourself once you complete this section.

[QR Code: https://www.av-test.org/fileadmin/pdf/security*report/AV-TEST*Security*Report*2018-2019.pdf]

Of the three operating systems we have been discussing, I would say that Linux offers the most security, privacy, and transparency due to its FOSS philosophy. The macOS, owing to various factors (market and non-market) probably takes second place, while Windows comes in a distant third on all counts.

However, if you were to rank them according to ease-of-use, macOS and Windows both rank higher than Linux. Linux also scores poorly in terms of user-friendliness of interfaces and overall design. Cost-wise, Linux systems win by a huge margin since Windows and macOS both required a paid license to run on your system.

The one thing that definitively sets Windows apart from the rest of the pack is the sheer number of (third-party) applications available for the OS. According to a post made on Windows Blogs (as linked via the QR code) in November 2018, there are over 35 million application titles with greater than 175 million application versions, and 16 million unique hardware/driver combinations. Just to present a comparison, Android and Apple only

have a couple of million apps each on their App stores.

[QR Code: https://blogs.windows.com/windowsexperience/2018/11/13/windows-10-quality-approach-for-a-complex-ecosystem/#LTW3DJvWw3d4cXb4.97]

All said and done, the one piece of advice I would definitely want you to take away from this chapter is this:

Always be aware of what programs are running on your system at ALL times.

If you find something suspicious or see something that you don't remember installing, ask the internet immediately! Honestly, spending a few moments to run a quick internet search on your preferred search engine is much better than spending hours to restore a system that has been overtaken by malware.

---

[1] Yeah, I'm explicitly saying that pirated software falls under the category of "Unauthorized software." I'll explain that in a bit.

[2] Applicable for all operating systems -- Windows, MacOS and Linux

[3] I'll tell you how to deal with browser plugins in a later chapter.

[4] Note, you can encrypt your files AND sandbox applications.

[5] Not available for Windows 10 Home version

[6] See above.

[7] The "Control Panel" is also available in the modern versions of Windows, i.e. Windows 8 & up. Simply search for Control Panel in your Start menu.

[8] I've chosen not to include QR codes that directly link to these tools, since they shouldn't be used on a whim. In any case, for the truly curious, they are merely an internet search away. Caveat Emptor!

BASIC (1 point)

First, make a list of all the important SaaS providers who are likely to have critical and/or identifiable information about you. I define critical and/or identifiable information is information that can be used to cause you physical, mental, or financial harm either directly or indirectly. For example, a silly nickname or poem on your profile may not seem very dangerous, but, in the wrong hands, it could potentially have multiple misuses.

Scan Your 'Public Profile': When you sign up with a SaaS provider, they usually ask you to enter some personal information -- usually your name, email address, and contact number. These details may then be made available to the general public through a public profile, especially in case of social networks. The information on your public profile is visible to the world and, by extension, to search engines. That means, anyone who happens to search your name on Google could end up seeing those details, should they choose.

Some social networks give you the option of keeping your profile private that is, most of the information you provide the social network is shared only with a chosen group of friends or followers and is not available to the general public.

I say most here because some information is still available under specific conditions. For example, Facebook allows you to hide your profile from external search engines, but some (or all) of it might still be visible to other Facebook users. Or, when you mark your profile as private on Twitter, your display name, ID, and bio are still visible. Same goes for Instagram, as well.

While I do believe that no is careless enough to reveal private information in their public profiles, it is surprising how many times I find a revealing tidbit casually tucked away in people's public profiles.

Chapter 9

Desktops-Browsers

INTERMEDIATE: (2 points)

Anonymize your 'Public Profile': Make a note of what information is visible in your public profile and ask yourself the question: How comfortable am I with people knowing this about me? If the answer to that question makes you hesitate, it is probably a safe bet that you might want to remove that from your public profile.

In fact, if it is not made mandatory by the SaaS-provider, I recommend NOT providing any personal information to these websites. You could try using a fake name, or share limited personal details only if/when absolutely necessary.

Tweak your Privacy Settings: Most SaaS websites will provide a specific link called Privacy Settings or something similar. Under this section, you will find all the options related to the public visibility of your personal data and activities.

IMPORTANT!!

Be aware that tweaking your privacy settings may have a significant impact on the way you experience the SaaS, especially in case of social SaaS.

If public visibility of your activities on the SaaS is not important to you, then I recommend setting your profile to private if the SaaS allows it. This will ensure that your activities are visible only to a limited set of users that you can control.

Some SaaS websites may also provide additional settings to tweak the visibility of specific behaviors on the website. For example, Facebook and LinkedIn allow you to choose which of your actions gets shared on your public profile.

Security settings: Most SaaS will also provide a specific link called security settings or something similar. Here, you can find options to reset your password and change your security question.

Use your preferred password manager and change your password to a more secure one, ideally with a length of 20 characters or more. Repeat this process every 3-6 months, at a minimum.

If the SaaS allows it, change the answers to your security questions to something non-obvious. For example, if your security question is, What was the name of your first pet? and your security answer is Fifi , change it to something completely random, such as your favorite Marvel character (Thanos) instead [2] .

If the SaaS allows it, enable multi-factor authentication (MFA) on your account. This acts as an additional deterrent for attackers trying to gain access to your account if your password gets leaked. Use one of the authenticator apps I recommended in the chapter on smartphones.

Note

Note that if you enable MFA, some websites/smartphone apps will ask you to provide your mobile number as a fallback alternative in case you don't have access to your authenticator app. I recommend doing this only for the sites you trust absolutely.

Payment information: There is a good chance that you have purchased something over the internet at some point in time. There is also a good chance that you paid for it using an online payment option such as a credit/debit card, netbanking, UPI or a third-party payment app. Almost all SaaS websites will offer you an option allowing you to store your payment information on their websiteas a 'convenience', but I would recommend against it.

Think about it, would you keep your wallet at your local kiraana just to avoid the hassle of carrying it to the shop every time? Then, why would you want to do that with a SaaS provider?

Look for the section that refers to payments, or wallet, or a similar term that might indicate the section where your payment information is stored. Delete any previously stored payment information.

If you have an active subscription with the SaaS website, you may be required to keep at least one payment method on file. In some cases, not having a payment method on file might result in stoppage of service. You need to make sure that the payment method you choose has an upper limit on spending -- whether through the SaaS settings or the settings of the payment method [3] itself.

This way, if a malicious actor manages to access your account somehow, any expense above the upper limit will be denied, and you'll receive a notification before any of your money is spent.

Introduction

You must be wondering, Isn't a browser just another software application? Didn't we already discuss software applications in the previous chapter?

You see, if the operating system is the primary agent between the user and the internet, the browser is the interface through which the user accesses the internet. Browsers belong to a special class of software applications since they are often the user's first window to the internet. Therefore, in this chapter, I will be discussing browsers as an independent entity with a separate set of privacy implications.

ADVANCED (3 points)

One way to enhance your privacy on a SaaS website to replace your details in the Privacy settings with random/anonymous data [4] . Note that, this does not erase/change anypast interactions logged with the SaaS website. For example, if you change your username on twitter, your previous tweets are still searchable using your old username, but the results will display your new username.

How do modern browsers work?

When you input data in your browser, you are essentially composing what is called a request packet. The browser then sends this request packet to the remote server, which analyses and computes a suitable answer. The remote server then sends back response packet(s) which is then displayed to you through the browser.

This request-response mechanism has been at the heart of internet browsing since the early days of the internet. Modern browsers not only provide an interface to stay connected with the world, but they also perform much more advanced tasks under the hood, while staying within the confines of this request-response mechanism.

Furthermore, reduced internet access costs and increased internet access speeds have resulted in modern browsers being increasingly used for various highly resource-intensive operations. These days, browsers have become an interface to access a multitude of powerful services such as serious (multiplayer) gaming, emulating entire operating systems, audio-video communication, to mention just a few!

Most websites are now mini-applications in themselves. Consider Google Docs, for example. There was a time when you needed to install a separate application (such as Microsoft Word) for your word-processing needs. Now, you can simply fire up your browser, visit the Google Docs website and create a new document --- just like that! What's more, all of the processing happens in the browser (and/or the remote server), and the document gets saved automatically to the cloud!

Sadly though, this change has not come without a cost. Modern browsers these days need to exchange a ton of data with the remote servers that host these websites, in order to present everything to you seamlessly. You already know that websites can (and do) ask your browser to share all kinds of data with them, ranging from the make and model of the browser to what devices are potentially present on your computer/device.

Since the browser always has full knowledge of both the request and response throughout a browsing session, it is highly critical that all data sent and received by the browser must be secured. Any leakage of data in this process has severe privacy implications and, therefore, every attempt must be made to prevent this data from being accessed by unauthorized parties.

In the sections that follow, we'll be looking at some of the more popular browsers, some not-so-popular ones, understanding what browser plugins and add-ons/extensions do, and how you can effectively use them to keep your personal data safe on the internet.

EXPERT (5 points)

If you're looking to become completely anonymous/invisible, then a good way to begin your anonymization journey is to delete any SaaS accounts that you don't use regularly.

Be warned that deleting SaaS accounts is often quite difficult and requires jumping through many hoops. There are a few companies that offer privacy protection services;that is, they track the internet for any presence of your identity and ensure that those mentions are removed. These services may either be do-it-yourself or paid or a combination of both.

A good place to start would be to check out the justdelete.me [5] service created and maintained by a bunch of volunteers, available here:

https://justdeleteme.xyz/

You can scan the QR code given to the right of this paragraph and open it in a browser on your device. This is a DIY service that provides you direct links to the delete account pages (and, in some cases, instructions) for deleting your account from various SaaS websites.

Popular browsers

The first graphical browser that was made available to the general public was called Erwise, and it was designed and developed as a student project at Helsinki University of Technology in 1992.

Today, however, the clear winner of the browser wars is Google Chrome -- a browser developed by Google that was quite a late entrant to the war. Google Chrome was first released in 2008 as a free browser for Windows users. It quickly gained popularity among the masses owing to its speed and clean, minimalistic interface – a popularity it still enjoys to this day, with a massive 70.71% of global market share on desktops and an equally massive 63.77% global market share across all devices, as reported by StatCounter.

Alternatively, you can check out Abine's DeleteMe service, which provides a similar (but paid) service for deleting your information from various data-brokers. Scan the QR code given to the right of this paragraph and open it in a browser on your device or go to:

[QR Code: http://gs.statcounter.com/browser-market-share/desktop-mobile-tablet/worldwide/#monthly-200901-201907]

Statistically, eight out of every ten Indians reading this book are likely to be regular Google Chrome users and (judging by what we have learned about Google so far) all eight of them have been sharing their data freely with Google all this time. It is also likely that they have made no changes to the default installation on their devices and that all these eight Indians will continue to use Google Chrome because, they are already so used to it, you know?

Privacy-aware browsers

If you are one of the eight Indians I referred to in the previous section and the thought of changing your browser makes you uncomfortable [1] , well, there's some good news for you.

Among some of the newer entrants trying to chip away at Google Chrome's market share are two browsers named Brave and Epic. Both of these are based on the Chromium open-source project (that is, they have the same look-n-feel) and use (almost) the same codebase as Google Chrome, except they don't send any data back to Google.

Brave browser

A relatively new entrant into the market, Brave browser has generated significant interest among privacy enthusiasts due to their strong stance on user privacy and their (intended) pay-to-surf model. Brave is completely open-source and they claim that their out-of-the-box installation settings are designed to be pro-privacy and anti-tracking, by default.

For instance, ad-blocking is made available by default in Brave. Or, the Safe Browsing option available in Chromium routes all safe-browsing requests to Google through a Brave-run server which doesn't keep any logs or store your IP. Brave also recently introduced private tabs with Tor for enhanced security and privacy while browsing.

Info

Brave's Pay-to-Surf Model

Yes, you read that right -- Brave intends to pay you to surf the web. The Brave Rewards program pays users in Basic Attention Tokens (BAT) for viewing ads from the Brave Ads program.

Brave claims that these ads are privacy-preserving and will be shown to Brave users in a non-intrusive and non-disruptive manner. Users will receive BATs (on a monthly basis) for viewing these ads. Brave Ads are opt-in by default and are matched directly to you on your local machine rather than a remote server, that is, your personal data never leaves your device. Brave claims that the only information they receive is accounting information to report campaign performance and delivery for advertisers.

However, there is no way to currently withdraw BATs and you can only spend them by donating them to your most visited websites or tipping content-creators who are Brave-verified, such as Wikipedia, and more. There are plans to allow users to withdraw their BATs into local currency or redeem them for real-world rewards but, as of August 2019, there is no clear date on when that is likely to happen.

[QR Code: https://brave.com/brave-rewards/]

https://www.abine.com/deleteme/

The fewer the number of accounts you have on the internet, the lesser are the chances of your personal information getting leaked by maliciousactors.

Epic browser

Like the Brave browser, the Epic browser is based on Google's Chromium project, but it is classified as commercial and proprietary software, that is, their source code is not open to review. While this may be a conscious decision to implement privacy-thru-obscurity, it goes against the spirit of transparency which is essential to be considered privacy-aware.

Epic also comes with extreme privacy enabled by default, including settings such as comprehensive ad-blocking, no history, no pre-fetching, no auto-fill, anti-fingerprinting measures, and many more. Epic also boasts of a one-click encrypted proxy to hide your IP address and encrypt your browsing. Furthermore, their privacy policy (rather uniquely) is written in plain English and mentions that usage data is neither collected from Epic browser nor stored on any servers.

While all of these features make Epic a mouth-wateringly lucrative option, the unavailability of source code is a huge flag that cannot be ignored.

The Tor browser

The name Tor has been adopted from the acronym for The Onion Router -- a worldwide network of servers initially developed with the US Navy to help people browse anonymously.

Using the Tor browser is akin to playing a game of Chinese Whispers over the internet; that is, it makes your request hop across multiple servers before routing your requests to the desired destination. The remote server responds back through the same path, thereby ensuring that your privacy is maintained behind a thick veil of whisperers . Since all communication is encrypted, none of the servers in the path can read it and, more importantly, none of it can (theoretically) be traced back to you.

To ensure this level of anonymity, Tor relies on a few basic principles:

Hides your identity: Tor does not ask for, store, or share any user data with any remote server

Removes trackers: Once you close the Tor browser window, all browsing history and data is erased.

Encrypted communications: All communication between the Tor browser, all the nodes along the route, and the remote server are end-to-end encrypted.

Due to the philosophies inherent in its design, Tor is the closest a browser can come in terms of achieving anonymity and maintaining your privacy on the internet, and I strongly recommend the Tor Browser for everyone wishing to surf privately and anonymously on the internet. There are a few downsides to using Tor, though.

Tor relays have often been abused by automated programs (a.k.a. bots) to harass and bring down websites anonymously. As a result, many websites have installed abuse prevention mechanisms in the form of human verification challenges (that is, CAPTCHAs and verification questions) that are presented to users accessing such sites via the Tor Browser. Users may find their browsing experience is noticeably slower than normal since the traffic hops across three different relays. Websites that automatically serve content based on your location will serve you content depending on the geolocation of your exit relay.

It may seem overkill to bounce your traffic through multiple different relays in different countries; it may be absolutely warranted in certain situations. Tor was primarily built for anonymity over the web. It was built as a tool for people to avoid tracking, for journalists to communicate without government interference, for law enforcement officers to track unlawful activities, for activists to escape surveillance -- essentially, Tor was built to help individuals seeking privacy and anonymity on an increasingly un-anonymous and heavily personalized web.

SaaS privacy concerns

If a SaaS website were to suffer a breach or if your username and password were to leak somehow, all of these details would lie exposed to *

anyone * who knows your username and password.

Of course, the onus is primarily on the SaaS provider to ensure that these security concerns are acknowledged and, if possible, addressed. However, you, as a user of the SaaS website, can also take some steps to mitigate the effects of a breach of privacy that might happen due to one of these concerns being realized.

To that end, here are some recommendations on evaluating a SaaS website on the basis of the various security and privacy concerns I outlined earlier in this chapter.

META

IMPORTANT!! Scoring Instructions for this section

You'll notice that the recommendations for each of the privacy concerns outlined in this section is exactly the same -- delete your account on the SaaS website or anonymize any personal details you may have provided them. You'll also notice that the evaluations questions require varying levels of knowledge of the associated subject matter.

That's why each section carries its own point value since the difficulty of the corresponding subject matter outweighs the simplicity of the recommendation.

All associated point values have been clearly stated next to each of the section titles.

Is Tor truly anonymous?

Short answer: Yes, and No.

Long answer: Any service that promises anonymity will always have adversaries looking to infiltrate it and the same applies to Tor, as well.

Tor primarily relies on a huge network of volunteers and organizations to run the Tor relays that constitute the Tor network. There is a very real possibility that one (or a few) of them could have already been compromised by adversarial actors -- either state or non-state.

In fact, in 2014, a coalition of government agencies managed to take control of many hidden Tor services and took down the notorious the deep-web drug marketplace, Silk Road 2.0, its proprietor, and 16 others in a high profile bust. In the aftermath of the news, a lot of people were left asking this very same question, Is Tor truly anonymous?

To their credit, the people behind the Tor project responded by posting a detailed blog post evaluating andanalyzing all the methods that could have been used to execute this high profile bust. You might want to read the whole thing over on their blog; it's titled, Thoughts and Concerns about Operation Onymous.

ToS and privacy policy (BASIC, 1 point)

Evaluate your SaaS by asking the following questions:

Did you easily understand the ToS and the Privacy Policy put forth by the SaaS?

Does the SaaS have a class A or class B rating on the ToS;DR website?

Can you import this downloaded backup to another, similar SaaS without requiring expert intervention?

If you answered no to one or more questions, then you may need to consider deleting/anonymizing your account on this SaaS website. Use one of the recommended actions mentioned in the previous section to either anonymize your personal details or delete the account associated with this SaaS.

[QR Code: https://blog.torproject.org/thoughts-and-concerns-about-operation-onymous]

The gist of the story is this: Over the years, Tor has faced multiple attacks by adversaries -- both state and non-state actors -- trying to infiltrate its systems through various means. While utmost care is taken to protect the hidden services, no system is 100% perfect. The government agencies in question probably managed compromise or commandeer some Tor relays and/or exit nodes which, combined with OPSEC mistakes committed

by the culprit, proved to be crucial in taking down the whole operation.

In other words, if a three-letter agency with (arguably) unlimited resources and singular interest in uncovering your secrets decides to take an interest, there's not much you can do, can you?]

Service reliability (ADVANCED, 3 points)

Evaluate your SaaS by asking the following questions:

Can you backup all of your data on this SaaS website and download it to a local machine?

Can you view the downloaded data without requiring advanced technical knowledge?

Can you import this downloaded backup to another, similar SaaS without requiring expert intervention?

If you answered no to one or more questions, then you may need to consider deleting/anonymizing your account on this SaaS website. Use one of the recommended actions mentioned in the previous section to either anonymize your personal details or delete the account associated with this SaaS.

Privacy settings

Regardless of which browser you use, there are a few settings that can be tweaked to achieve a higher level of privacy and anonymity from websites attempting to profile you and your browsing habits. I strongly recommend that you spend some time working through this section -- especially if you haven't changed any settings on your browser since the day it was installed. If left unchecked, default installations of all popular browsers are designed to share a lot of data about you and your browsing habits, with their respective remote servers.

In the following sections, I provide you with a list of the most important browser settings that need to be changed to enhance your privacy while using your preferred browser.

Security and transparency (EXPERT, 5 points)

Evaluate your SaaS by asking the following questions:

Do the SaaS offer a bug-bounty program for ethical hackers?

Does the SaaS regularly provide security updates and proactively disclose security incidents?

Does the SaaS proactively deploy the latest security practices and phase out older ones regularly?

If you answered no to one or more questions, then you may need to consider deleting/anonymizing your account on this SaaS website. Use one of the recommended actions mentioned in the previous section to either anonymize your personal details or delete the account associated with this SaaS.

Private windows

One of the simplest changes you can make to your browsing habits is to use the privacy-aware browsing mode in your browser. This mode goes by different names for different browsers -- Chrome calls it Incognito , Firefox calls it Private , and Edge (as well as IE) calls it InPrivate . Whatever the name, the idea behind the concept remains the same -- this mode provides the user with a browsing session in which all of the information sent and received within the session is completely erased at the end of the session.

Security breaches and response (INTERMEDIATE, 2 points)

Evaluate your SaaS by asking the following questions:

Has the SaaS suffered a data-breach any time during the time it has existed?

Did the hear about it from an official account or from a third-party?

If data was lost or stolen, was the SaaS website able to recover both the data and the trust of its users?

If you answered no to one or more questions, then you may need to consider deleting/anonymizing your account on this SaaS website. Use one of the recommended actions mentioned in the previous section to either anonymize your personal details or delete the account associated with this SaaS

Telemetry opt-out

All three of the most popular browsers in use today -- Google Chrome, Mozilla Firefox, and Safari – have some kind of tracking or telemetry enabled out of the box. All of them claim that any and all telemetry data sent to them is anonymized and collected mainly to improve performance. I think you should be at least made aware that you have the option to opt-out of it.

Security updates (EXPERT, 5 points)

Evaluate your SaaS by asking the following questions:

Was the SaaS affected by any of the superbugs that were recently discovered?

Did the SaaS take immediate steps to mitigate the threat resulting from the superbug being available openly in the wild?

Did the SaaS roll out patches and/or switch to more secure alternatives?

If you answered no to one or more questions, then you may need to consider deleting/anonymizing your account on this SaaS website. Use one of the recommended actions mentioned in the previous section to either anonymize your personal details or delete the account associated with this SaaS

Syncing and personalization

All popular browsers provide the option of syncing your activities on the browser with the cloud. If you are logged in, your browser will offer you the option of storing one or more of the following -- your bookmarks, your history, your open tabs, your logins, your extensions, and settings -- from your browser, in the cloud. The advantage of syncing all this data is that it helps you maintain a uniform browser interface by syncing with the cloud. However, it also means you are sharing all of that data with a third-party that may or may not be able to keep this data absolutely private.

While it is extremely tempting to keep everything synced to the cloud, I recommend that you only sync the extensions and settings, if you absolutely must. I strongly recommend AGAINST logging in and/or syncing your data, for obvious reasons or privacy and anonymity.

Data access (ADVANCED, 3 points)

Evaluate your SaaS by asking the following questions:

Where are the remote servers for the SaaS located?

Have any of the local governments tried to petition the SaaS for user data?

Has the SaaS transparently revealed what user data was turned over to authorities?

If you answered no to one or more questions, then you may need to consider deleting/anonymizing your account on this SaaS website. Use one of the recommended actions mentioned in the previous section to either anonymize your personal details or delete the account associated with this SaaS.

Search engine integration

So powerful is Google's presence and reputation as the best search engine on the internet that all the popular browsers use it (that is, Google) as their default search engine. Although this reputation is well-earned, due to the quality of search results it offers, you must also remember that Google collects massive amounts of data every time you use their search engine. Therefore, I recommend using a more privacy-aware alternative [2] , such as DuckDuckGo or Qwant .

Furthermore, when you type in the address bar of the browser, you'll notice that your browser offers instant suggestions that appear as you type. This is because your browser sends everything you type, as you type to a search engine and retrieves those suggestions.

Conclusion

When it comes to creating accounts on SaaS websites, the saying, Less is more is probably the perfect recommendation anybody could give. Whenever a new website or a new service is announced, we often feel the need to rush and reserve a unique identity on that website or service for ourselves, just so that we don't miss out on it.

I'll be the first to admit that the desire to own your own unique piece of the internet real-estate can be overwhelmingly tempting. However, every new identity you create on the internet erodes your chances of staying anonymous and further adds to the risk of leaking your personal information. Every new public profile means an additional tidbit of your data gets added to the internet. It means that the data-brokers on the internet get to add another piece to the jigsaw puzzle that is your identity.

Signing up for a new SaaS website just because all the cool kids are doing it is a bad idea. Unless you can ensure complete anonymity with every sign up, I'd recommend that you refrain from signing up for accounts that you don't really need.

I mean, is it really important that you get the username cooldude69 before someone else does?

---

[1] For instance, with email, phishing is a kind of an adversarial attack that relies on the weakness of the user rather than a specific vulnerability of the email website portal itself. The login information is (unknowingly but) ‘willingly’ provided by the user to the adversary in the course of the attack.

[2] You can add this information as a note in the password manager itself. That way, you don’t have to remember this information and it is still available whenever you need it.

[3] If your banking app allows it, you can create a separate wallet with limited amounts specifically for the SaaS to ensure a hard upper-limit on spending.

[4] Although, some sites like Facebook insist on a real-name policy and do not take kindly to fake/anonymous/random names, so beware!

[5] The original service is still available at justdelete.me and is still operational, although it seems to be under the control of BackgroundChecks.org

Cookies, tracking, and content blocking

Every website you visit stores a small text file on your computer called a cookie . This text file contains information about you, your system, and some data about your visits to the website. Some websites may also store third-party cookies (i.e. cookies from other websites, usually advertisers and/or social networks) on your system. Advertising networks use these cookies to track the user on multiple websites and gather their browsing information.

Cookies are the reason why you don't have to re-login when you accidentally close the browser tab or window. Cookies are also the reason why a specific ad keeps popping up no matter which webpage you open. Thankfully, all modern browsers provide an easy way to block third-party cookies.

Chapter 12

Networks: Connectivity and Internet

Forms and autofill

Over the years, forms have become an integral part of web browsing - in fact; we use forms without even realizing that we are using them! For example, when you login to a website, you are actually submitting a login form to the remote server, which then validates it and responds accordingly. Or, for example, when you buy something from a shopping site, you fill out a form with payment details, shipping address, and other relevant information. Most modern browsers have a form autofill feature that allows you to save time and fill out various forms at the click of a button.

Introduction

While the most common metaphor for the internet is a series of interconnected tubes , a better metaphor would be that of an open bazaar. The websites are stalls, and everyone uses the services of a translator to speak the language of the sellers. All conversations, transactions, and interactions happen through the translator. Since you can't speak the language yourself, you can only hope that your translator is honest with you.

You may have figured out by now that the translator in this analogy is the network over which your devices communicate. The network protocol is analogous to the language used by the translator and the information you provide the translator may or may not always remain private; for all you know, the translator may be wearing a hidden mic!

So, how do networks function?

When it comes to transmitting data over the internet, networks have a pretty simple job -- to carry information from one point of the network to the other. Most descriptions of networks portray the concept as foot-messenger ferrying letters to and from different addresses.

However, the actual execution is a lot more complicated. Since the network has no memory, that is, it has no way to remember what a device looks like. Instead, the network actually relies heavily on the device identifying itself accurately and honestly.

Surprised? Here, look at how the foot-messenger scenario * actually * looks like in terms of information being sent over a network:

You write a letter, put it in an envelope, write the address, and give it to the foot-messenger.

The foot-messenger takes the letter and knocks on every door that they can find, gives them a copy of the letter and asks them if the address refers to their house.

Every house is expected to answer the foot-messenger’s question truthfully. If they are not the rightful recipient, they are expected to trash the letter immediately.

Once the foot-messenger finds the right house, they deliver the letter and wait for a response.

The foot-messenger takes the response letter and knocks on every door that they can find, gives them a copy of the response letter and asks them if the address refers to their house.

Every house is expected to answer the foot-messenger’s question truthfully. If they are not the rightful recipient, they are expected to trash the letter immediately.

Once the foot-messenger finds the right house, they deliver the response letter and wait for the next letter to be delivered.

I hope you can see the inherent privacy issues in this communication design.

A device may choose to misrepresent itself as the rightful recipient of a message.

The foot-messenger (or their evil twin) may themselves read the contents before proceeding to the next step.

These two scenarios are the primary attack vectors to keep in mind when considering the privacy issues within the network. I'll discuss them in further detail in the #RohitRecommends section of this chapter.

Permissions andsite settings

The internet is accessed by a wide variety of devices with a wide variety of hardware. Most modern browsers are increasingly equipping themselves with various interfaces that can take full advantage of the various capabilities of your device. Thismeans browsers can now request to access location information.

Note

Remember all that data acquired from your phone in the first chapter? Well, a huge part of it was thanks to the fact that your phone browser runs JavaScript. With JavaScript and the modern browser, developers can make the browser do a lot of powerful things – both useful AND nefarious.

Therefore, under ideal circumstances, I'd recommend that you toggle JavaScript to Blocked as well. However, the vast majority of websites on the internet rely on JavaScript to provide many of their features and blocking them from using JavaScript often breaks their functionality. Toggling this setting to Blocked would significantly alter your browsing experience, so I'm going to recommend that you leave it as it is.

Plugins and extensions

Imagine, for a moment that you have just purchased a house. It is big, roomy, empty and it doesn'thave a garage. If you decide to build a garage, then you have extended the house. If you decide to add a utility such as air-conditioning or central heating, you have plugged in an additional component to your house. The extended garage can also utilize the air-conditioning' plugin.

While browsers are powerful applications in their own right, their utility can be further enhanced by the use of plugins and extensions.

Info

Extensions? Add-Ons? What's the difference?

Short answer: For this book, there's (essentially) no difference.

Long answer: Google Chrome and Safari both call them extensions, whereas Firefox, Internet Explorer and Edge refer to them as add-ons, but they all imply the same thing. Firefox uses the umbrella-term Add-ons under which extensions, themes, language packs, etc. are further separately classified.

I have used the term extension through this book to avoid any confusion, but I'd like to clarify that I mean the same thing whether I say extension or add-on .

Wired networks

Wired Networks connect devices to each other and the internet using physically wired connections.

Typically, wired networks are seen in homes, offices, and cyber cafes and they make use of Ethernet cables, network adapters, and routing devices (such as hubs, switches, or routers) to share a single internet connection with other devices on the same network. Connections to the internet may be made over broadband, ADSL, or fibre-optic network depending on the technology employed by the ISP providing internet access.

For instance, local ISPs typically provide internet over LAN or cable broadband, whereas ISPs like JioFiber, Airtel, andmore utilize their own fibre-optic network to deliver internet to your home. Wired networks typically offer superior performance as compared to wireless networks but at the cost of portability.

The difference

Wireless networks

Wireless networks connect devices using electromagnetic waves following a specific communication standard such as Wi-Fi 802.11, GSM, Bluetooth, and more. Wireless networks are typically used in homes, offices, and public places and they can be used to provide users with internet connections on their portable/handheld devices.

Plugins and extensions are fundamentally different

A plugin is an additional piece of software (usually third-party) installed alongside the browser that provides specific functionality excluded in the default browser installation. For example, when you watch Netflix videos in your browser, your browser usually invokes the Widevine Content Decryption Module -- a plugin that enables playback of encrypted media within the browser. Or, when you used to play flash games in your browser, you were actually invoking the Adobe Flash Plugin to perform this task.

An extension, on the other hand, is a (sort of) middleware that enhances the browser capabilities either through customization or manipulation of data received and processed by the browser. When you activate an adblocker extension, it processes the data received by your browser and performs its function, that is blocking ads.

In other words, an extension may sometimes invoke a plugin in the process of carrying out its tasks, but a plugin is always a standalone object that provides very specific functionality.

Wi-Fi/WLANs

Most homes and offices employ the 802.11 Wi-Fi or Wireless LAN (or WLAN, for short) which involves sharing the internet connection acquired over a wired network by using a wireless internet router. However, thanks to recent technological developments, telecom services providers now provide their customers with hi-speed 4G LTE networks, with browsing and downloading speeds comparable to (or better than) most WLAN/Wi-Fi and Broadband speeds.

Wireless networks suffer from the problem of reliability because they are subject to interference from other electromagnetic emitters and also because of theoretical limits on their propagation, strength, and carrier capacity. Wireless networks, especially WLANs, are also less secure as compared to their wired counterparts, as we will see in the next section.

Potential security concerns with plugins

For a long time, browsers would depend on various plugins to execute some fairly processing-intensive tasks, such as loading embedded games, applets, or videos inside the browser window. It was fairly common to have browser invoke the flash plugin to play games and videos or invoke the Java plugin to display an applet. Being able to experience multimedia in your browser usually meant running one of these plugins in the browser window.

However, this capability came at significant risk -- these plugins often had security vulnerabilities that could be (and often, are) exploited by attackers to gain control over your system. Furthermore, since these plugins were maintained, updated, and released independently, updating them was often a separate process. Thus, anyone who chose/forgot/refused to update the plugin was instantly vulnerable to attacks that exploited the plugin's vulnerability.

Info

Flash was one of the biggest culprits in this regard with nearly 900 severe (that is, CVSS score >= 9) exploits discovered and published between April 2008 and May 2019, as per the listing available on www.cvedetails.com

In fact, in 2010, the frequent discoveries of Flash vulnerabilities even prompted Steve Jobs to declare that Apple would stop allowing Flash on iPhones, and he wrote a blog post titled Thoughts on Flash on the official Apple blog (QR code given alongside this paragraph) in 2010.

GSM

GSM stands for Global System for Mobile communication, and it is the wireless protocol on which 2G, 3G, 4G LTE, and 5G is delivered to compatible devices. GSM provides end-to-end security and confidentiality of the subscriber by assigning temporary ID numbers and applying advanced techniques such as robust encryption algorithms, and frequency-hopping to maintain the privacy of the communication.

However, its encryption was leaked in 1994, and multiple vulnerabilities have since been discovered that indicate that GSM is as susceptible to

intrusion and malicious attacks as any other wireless network.

[QR Code: https://www.apple.com/hotnews/thoughts-on-flash/]

In July 2017, Adobe finally announced that it would end support for the Adobe Flash plugin by 2020 and encourage the use of open HTML5 standards instead, as seen in this official blog post titled Flash & The Future of Interactive Content on the Adobe Blog. Scan the QR code given alongside this paragraph to read the entire blog post on your device.

Bluetooth

Named after a tenth-century Norse king Harald Bluetooth, this technology was primarily conceived as a low-cost, low-power method to develop wireless headsets that could transmit and receive data over short distances, short-wavelength UHF radio waves. The most popular implementation of Bluetooth is the wireless control and communication between mobile devices and receiving units such as headsets, vehicles, and other devices.

Although versions of Bluetooth after version 2.1 have better encryption protocols, several vulnerabilities have been discovered in various implementations, since as early as 2001.

[QR Code: https://theblog.adobe.com/adobe-flash-update/]

Modern browsers have already begun the process of replacing these plugins by adopting open standards and encouraging alternative languages and technologies. The uniform adoption of open standards has allowed web developers to create amazing, fun, and useful applications without having to rely on proprietary code, such as Adobe Flash, Shockwave, Java, and many more.

NFC

The Near-Field Communications (NFC) protocol relies on proximity or taps from/to other NFC-enabled devices to conduct a transfer of data. Connections between these devices are established automatically without any password or credential requirements.

Potential security concerns with extensions

While plugins are bits of (usually proprietary) third-party code running within the browser, extensions are bits of code that usually perform certain tasks on the web page before it is displayed (or while it is being displayed) to the user. For example, uBlock Origin is an adblocking extension which scans webpages received by your browser and removes ads from the page. That said, everything that I have said in the previous paragraphs about plugins is also somewhat applicable to extensions.

If you are thinking, If an extension can access all webpages, then it means the extension has access to everything I view while it is installed, which means my browsing history is not private at all!, you would be absolutely right. Malicious extensions can disguise themselves and quietly siphon away your data in the background -- a recent leak of private FB messages from 81000 accounts was carried out in this manner.

Tips

While installing extensions…

There are a wide variety of extensions and add-ons available for your browser, and it is important that you choose carefully the extension you want to install. To that end, I have compiled a few simple rules of thumb you must follow while installing extensions for your browser:

Trust and verify: Always install extensions only from trusted, vetted, and verified developers and sources. Google has a vetting policy (called Project Strobe) for extensions on the Chrome Web Store to ensure that all extensions on the Chrome Web Store are trustworthy by default. Mozilla uses the Recommended Extension badge to indicate that the extension has undergone a security review.

Everything in moderation: Only install the extensions that you absolutely need and use. The more the number of extensions on your system, the greater are the chances of one of them going bad or rogue and infecting your system.

Prefer open-source extensions: Even if you can't read code, people who can, will usually quickly shut down (or fork away from) extensions that have malicious code, thus inoculating you from any potential harmful effects.

Eternal Vigilance: Keep your extensions up-to-date and ensure that its code continues to remain uncompromised. Good extensions can very quickly turn bad, for example, in 2017, the Web Developer extension for Chrome was hijacked, and a malicious update was pushed out to users which caused ads to appear during browsing sessions.

Common attack vectors

In the introduction to this section, I compared the network to a bazaar and the network adapters to a translator/guide helping you communicate with a seller in the bazaar. It is easy to see how your privacy can be compromised if the translator were to, somehow, go, rogue.

In this section, we will look at some commonly used attack vectors for network adapters and routing devices that can be used to compromise your privacy over the internet.

RohitRecommends

By all accounts, Google Chrome is the browser of choice for most people surfing the internet, leaving all other browsers far behind. Indians, too, overwhelmingly choose Google Chrome as their browser of choice, with 81.15% market share on the desktop and 66.4% market share across all devices.

While there are ways to make Google Chrome more privacy-aware, I would recommend avoiding it instead. Due to the business model they have implemented, the entire Google ecosystem is designed to give you as little privacy as possible. Therefore, in my opinion, the less you use Google products, the better it becomes to maintain the privacy of your data.

Therefore, most of the recommendations in this section will be made under the assumption that you are NOT using Google Chrome. Wherever possible, I will try to include relevant options for Chrome, but I do NOT endorse it. Furthermore, some of my recommendations for Mozilla Firefox will also apply to Google Chrome, although the wording involved may be different from what you'll read in this book.

Important!!

In the sections that follow, there will be a lot of recommendations which will feel extremely overwhelming at first glance. You might even think, That's a lot of work for just a few points! and, technically, you would be absolutely right.

Which is why, I propose a 5x multiplier for each recommendation level, valid ONLY for this chapter.

How does that sound? Good? Okay then, open your browser and start earning your points!

Identification

One of the most important aspects of planning an attack on a network device is acquiring information on the target. This involves figuring out the identity of the target and searching the target for weaknesses and vulnerabilities. The more information you have about a target, the better you can plan your attacks. Not surprisingly, there are a bunch of tools and techniques that can be used in this phase of operations, that is, to identify the target and its vulnerabilities. The most common among them are:

Port scanners: These are specially designed programs to identify open ports on a device. An open port can indicate a specific protocol being employed by the device and any vulnerability applicable to that protocol can then be used to gain entry into the target system. Think of this as an open door (or window) through which customers can enter or communicate in our bazaar analogy.

Packet sniffers: Packet sniffing is an eavesdropping technique where the attacker is able to intercept all your communication without your knowledge or permission. This is actually much easier than it looks because of the way networks are designed. An attacker can intercept all the data being sent to your device by deploying their adapter in promiscuous mode on your network. To use the same bazaar analogy, this would be like someone being able to clearly monitor each and every interaction between the customer and the shop.

Deep Packet Inspection (DPI): This is a highly-intrusive packet-sniffing technique that involves using automated programs to read the contents of the datapackets that are being exchanged between your computer and the remote server. DPI can be used to extract sensitive information about the victim's online activities and browsing habits. This knowledge can then be used to create a firewall that can interfere or interrupt such traffic, as and when necessary.

It is common knowledge that such DPI-assisted firewalls have used by some authoritarian governments to monitor the activities of their citizens and (either proactively or reactively) curb their freedoms. In recent times, a few ISPs have also taken to using DPI to analyze network traffic and snoop on their users without their knowledge or permission.

Spoofing: Spoofing involves impersonating either a device or an authority to con the victim. In a MAC-spoofing attack, a malicious attacker might impersonate your MAC address to gain entry into your local network, or to install software that works only with certain MAC addresses.

In an IP-spoofing [1] attack, a malicious attacker crafts packets with a false source IP address to fool the victim into sending critical data to the attacker's desired destination. In a DNS-spoofing attack, malicious actors may change DNS entries pertaining to a website either on your local machine or on your network's DNS server, in order to redirect you to the attacker's computer and steal your credentials.

War-driving: This term refers to reconnaissance techniques where malicious attackers attempt to surveil a geographical area to identify available access points physically. Malicious attackers physically drive around with a portable/handheld device to scan areas and map out all the available Wi-Fi access points into a database.

BASIC (5 points)

Interception

The interception phase is the phase of an attack by a malicious actor that actually threatens your privacy and your personal data. Some malicious actors may choose an interruption phase instead of interceptions , which aims to disrupt a user's online activities completely.

The actual attack perpetrated by a malicious actor takes the form of either an interception or interruption of the flow of data. Both of these techniques have different end-goals; while interceptions are aimed at acquiring critical information, interruptions are mainly intended to be disruptive. To extend our bazaar analogy, an interception would be if someone were recording everything said by your translator/guide and interruption would be a crowd screaming gibberish while your translator was trying to establish a communications channel with the seller in the bazaar.

Let's look at some of the most common interception and interruption attacks:

Man-in-the-Middle: Also known as Monkey-in-the-Middle and usually shortened to MitM, these attacks involve a malicious actor who is in a position to intercept communications between two networked devices, such as your PC and the remote server. Information sent by one device is intercepted by the man in the middle, that is, the attacker (thus the name) before being passed on (usually after changing it in some manner) to the other device. For an MitM attack to be successful, the attacker must be able to impersonate both devices on either side precisely.

Replay attacks: These are a lower-tier of the MitM attack, where the attacker silently intercepts communication between two devices on a network and replays relevant portions at a later time with the intention of impersonating one of the two devices. For example, replay attacks can be used by a silent MitM attacker to re-login to a user's account after they log out. Or, an actual replay of a user's voice could be used to breach a voice-recognition system.

Smurfing/Flooding: This is a form of Denial of Service (DoS) attack employed by malicious actors to overwhelm a device or adapter on a network. It involves sending a large number of IP-spoofed communication packets to multiple devices on a network. When all these devices reply back to the spoofed IP, the victim's machine slows down to an extent where it becomes difficult to work on it. The Ping flood and Ping of Death attacks are essentially variations of the Smurfing attack.

Browser recommendation

I recommend using any of Mozilla Firefox, Safari, or Brave [3] since all three of them (seemingly)provide several additional ways for users to tweak their privacy settings.

Both Firefox (and Safari) have a good track record in terms of user-privacy and data-security, until now. Firefox is developed and maintained by Mozilla -- a non-profit organization -- who claim that their mission is to keep the internet open and accessible to all. Safari, on the other hand, is the default browser that comes bundled on all Apple devices, and it follows Apple's privacy and security philosophy in its design.

A recent analysis of popular web browsers posted in July 2019 on the ExpressVPN blog ranked both Safari and Firefox higher than Google Chrome. Scan the QR code displayed alongside to read the article titled Ranked: Security and privacy for the most popular web browsers in 2019 on the ExpressVPN Blog.

[QR Code: https://www.expressvpn.com/blog/best-browsers-for-privacy/]

I'll be outlining these tweaks shortly, so make sure that you apply those tweaks if you want to optimize, the privacy of your personal data.

Info

Why not Tor, instead of Firefox, Brave, or Safari?

Ideally, using the Tor browser would ensure maximum anonymity and, therefore, maximum privacy. However, remember that Tor has the unfortunate effect of slowing down your browsing speeds -- not recommended if there are important tasks to be done in a hurry. Furthermore, logging in to an online account (any account) while using the Tor browser actually compromises your privacy, if you've logged into the same account from other browsers.

Essentially, what I'm saying is, if you're using the Tor browser, use it independently from other browsers, that is, that is, stuff that you do in the other browsers and stuff that you do in the Tor browser should be kept separate and exclusive.

Wireless attack vectors

While the above attack vectors can be (and often are) used for both wired and wireless networks, there are some attack techniques specific to wireless networks that deserve a special mention:

Malicious networks: Malicious networks are usually created by craftingaccess points that are specifically placed by a malicious attacker to lure unsuspecting victims. Theseare typically waterholes , that is, networks placed and presented in such a manner as to lure the user into connecting to them. Typically, such access points are given lucrative names such as Free Airport Wi-Fi or Free Hotel Wi-Fi and are always unsecured and/or unencrypted.

In some cases, the attacker may even smurf, flood, or jam other SSIDs to further influence unsuspecting victims. Once connected, devices are rendered immediately vulnerable since all communication must pass through this malicious network, thus providing the attacker with a clear MitM view of all the unencrypted traffic.

Evil twin attack: An evil twin attack is quite similar to a malicious network except that it is specially crafted to impersonate a previously connected Wi-Fi AP. The evil twin is the Wi-Fi equivalent of the phishing scam. By conducting a war-driving exercise, a malicious attacker identifies unsecured Wi-Fi access points (APs) and then creates an evil twin for one of the chosen APs.

Sometimes, attackers may also reverse engineer evil twin APs by intercepting the Wi-Fi search scans made by the victim's device to see what other APs the user is trying to probe [2] . If any of them are unsecured, the attacker may use those names to create an evil-twin for the victim.

In either case, the original AP is then smurfed, flooded or jammed while keeping the evil twin alive. Since the evil twin has the same SSID, any devices connected to the original AP can be made to switch to the evil twin thus giving the attacker a clear MitM view of the communication between the user and any remote servers they may be connected to.

WEP/WPS brute-forcing: Brute-forcing refers to the practice of trying out every possible combination of alphabets, numbers, and special characters to break the encryption and find the password to a secured wireless network. A variant of the brute-force attack (and one that is increasingly more commonly used) is the dictionary attack in which the most commonly used passwords are tested first before attempting a pure brute-force attack. WEP is an older form of encryption used by Wi-Fi routers and has since been discovered to be extremely vulnerable to the simplest brute-force attacks. In some cases, WEP-encrypted passwords have been cracked in as little as 5 minutes.

WPS or Wi-Fi protected setup relies on pairing devices by simply pressing a button on two Wi-Fi devices. The encryption, in this case, uses an 8-digit PIN to encrypt the information exchanged between the devices and set up a WPA link. However, a tool called Reaver can brute-force the WPA-encryption without the physical WPS button being pressed. While WPA by itself remains a somewhat secure encryption method, the WPS encryption key has been proven quite susceptible to brute-force attacks by the Reaver tool.

Note that, given a bit of time, money, and patience, brute-force attacks can also be used to recover passwords encrypted using strong(er) encryption such as WPA and WPA2. Open-source tools such as aircrack-ng have made the entire process as simple as downloading a file, extracting it, and running it on your system!

Jamming: Jamming is a more aggressive DoS attack in which the RF frequencies (on which the wireless signal operates) are jammed using external interfering signals. A simple example of inadvertent jamming is the sudden loss of Wi-Fi when the microwave is switched on. Malicious attackers may use this technique to induce artificial jamming and then lure unsuspecting victims with a rogue AP or an evil twin attack.

Note

All of these wireless attack vectors are applicable for the other types of wireless protocols as well, that is, GSM, CDMA, Bluetooth, and NFC. Ever since the design for GSM encryption was leaked in 1994, various security researchers have been able to employ most or all of the aforementioned common attack techniques such as packet sniffing, jamming, smurfing, and different kinds of MitM attacks.

Private browsing

Regardless of whether you are using Google Chrome, Mozilla Firefox, Safari, Brave, or any other variant, I recommend using the privacy-aware browsing mode for any and all kinds of casual internet browsing.

This is because no data (such as history, cookies, and many more) is stored in such private browsing sessions. So, if you use a shared computer at home, work, or anywhere, I recommend that you always use the privacy-aware mode.

However, do remember that the privacy-aware browsing mode does not make you truly anonymous in any way. It merely prevents other users of the same system from being able to see any activities conducted during this browsing session. Your network administrator, your ISP, any websites you visit, and any people physically next to you will still be able to see and track what you do during this privacy-aware browsing session.

To open a privacy-aware browsing window:

In Firefox: Use the New Private Window option in the hamburger menu on the top right or press Ctrl+Shift+P in an existing Firefox window. A new window will open informing you that You're in a Private Window .

In Safari: Use the New Private Window option in the File menu on the top right. A new window will open informing you that You're in a Private Window .

In Chrome: Use the New incognito window option in the three vertical dots menu on the top right or press Ctrl+Shift+N in an existing Chrome window. A new window will open informing you that You've gone incognito .

Note

Safari does not have a keyboard shortcut to open a private window but you can assign one manually by going to System Preferences | Keyboard & Mouse and clicking on the Keyboard Shortcuts tab.

Bluetooth

There exist several different attack vectors for the Bluetooth protocol, not all of which bear resemblance with the more generic wireless attack vectors described in the section above.

Here are a few popular Bluetooth attack techniques commonly employed by malicious attackers:

Bluejacking: Bluejacking, by itself, is a relatively benign Bluetooth attack that involves sending unsolicited messages to nearby Bluetooth devices. The malicious variant of a bluejacking attack involves sending the contact file (usually a VCF file) to an unsuspecting victim. If this contact file is added to the phonebook, any files sent by the contact may be automatically opened by the device, thus elevating a simple bluejacking attack into a backdoor attack.

Bluesnarfing: Bluesnarfing involves unauthorized exploitation and theft of information from a wireless device through its Bluetooth connection. Attackers may download your contact list, your calendar, and other sensitive data using your device's Bluetooth connection.

Bluebugging: Bluebugging involves completely taking over a victim's mobile phone by acquiring unauthorized access via its Bluetooth connection. Attackers will often pose as a known Bluetooth device (for example, your headphones) and attempt to pair with your Bluetooth device. Once connected, the attacker acquires full control over your phone and can use your phone to place calls, listen to calls, read messages, read emails, use your phone as a modem, and even track your location!

Blueborne: Possibly the most dangerous attack vector, Blueborne was a comprehensive security threat that exploited multiple vulnerabilities in the Bluetooth protocol. A phone targeted using Blueborne could be completely hijacked with no user interaction, […] and does not require any preconditions or configurations aside fromthe Bluetooth being active.

Blueborne affected almost all devices, from phones to audio systems to desktop PCs across multiple vendors, including Google, Microsoft, Apple, Amazon, LG, and Samsung -- just to name a few. All of the vendors involved immediately patched the vulnerabilities that were revealed, but unpatched devices could still be vulnerable to Blueborne attacks.

Note

Technically, even though Bluetooth can be considered a wireless network, it is treated differently (by developers and attackers both) due to the way its protocol is designed.

NFC

Drive-by: You may have seen the video of the man in a convenience store making a payment by tapping the payment device to an unsuspecting

user's back pocket, where the victim's contactless card was probably kept in a wallet. If you haven't, you can check it out here:

Privacy settings

Once you have chosen your preferred browser, we'll need to ensure that your browser settings are optimized for the best data-privacy possible while ensuring that your browsing habits remain unaffected. In order to achieve this, I'll be recommending a few changes that you will want to make in the Settings [4] (or Options , or Preferences) of your browser to ensure the privacy of your data.

Important!!

The recommendations that follow are specific to Mozilla Firefox, but the overall philosophy is applicable to some of the other browsers as well. I'll try and cover a couple of other browsers, but I strongly recommend switching to Mozilla Firefox.

Mozilla Firefox

First, ensure that your Firefox installation is absolutely up-to-date by going to Menu | Help | About Firefox. A small window will pop-up telling you whether Firefox needs to be updated. If it does, download and install the update and then restart the browser for the changes to take effect.

Once you have updated your Firefox browser to the latest version, go to Menu | Options or type about:preferences in the address bar of your Firefox window and press Enter . Then, one-by-one, follow all of the recommendations listed below:

Opt-out of telemetry and collection of usage data: Click Privacy & Security in the sidebar, scroll down to the section titled Firefox Data Collection and Use and uncheck the checkboxes titled:

Allow Firefox to send technical and interaction data to Mozilla.

Allow Firefox to send backlogged crash reports on your behalf.

Turn off syncing and personalization: Click Sync in the sidebar and check if you are logged in to your Mozilla account. While it is extremely tempting to keep everything synced to the cloud, I recommend that you only sync the extensions and settings, if you absolutely must.

Change your default search engines: Click Search in the sidebar and in the dropdown available under Default Search Engine, switch to a more privacy-aware alternative such as DuckDuckGo instead of Google. Click the link titled Find more search engines under the One-Click Search Engines section to search for and add additional search engines.

Search suggestions: Disable the search-as-you-type (or search suggestions) feature by unchecking the checkbox next to Provide search suggestions .

Cookies, tracking, and content blocking: Click Privacy & Security in the sidebar and under Enhanced Tracking Protection , choose Strict for better protection of your browsing data. I also recommend Always choosing under the Do Not Track setting.

Permissions and site-settings: Click Privacy & Security in the sidebar, and, under the section titled Permissions :

1) One-by-one, click on each of the Settings buttons next to Location, Camera, Microphone , and Notifications and select the checkbox titled Block new requests to access [XYZ] , where [XYZ] refers to the feature whose settings are being looked at.

2) Click on the Settings button next to Autoplay and change the Default for all websites to Block Audio and Video in the dropdown.

3) Next, select the checkboxes next to Block pop-up windows and Warn you when websites try to install add-ons .

Once you've completed the recommended actions above, go through the list again and see if there is anything you (or I) may have missed. Mozilla may have added new privacy features to Firefox between the time this book was written and by the time you are reading this. If you find something not covered in this set of recommended actions, I suggest you look it up on the internet and see how it impacts your privacy.

The book's companion website (privacy.clinic) will also have regularly updated information about how to best tweak your browser settings for optimal privacy.

Info

Firefox Lockwise

Firefox Lockwise is a password management tool that helps you generate, store, and autofill passwords using your Firefox browser. Initially named Lockbox, it was first made available as a separate extension in 2018. It was renamed to Firefox Lockwise and integrated with the browser as a core feature replacing the existing Password Manager in version 70.

Since it is a relatively new addition to Firefox at the time of writing this book, the jury is very much out on the security and privacy aspects of Firefox Lockwise. Especially, for those of you who are already using a password manager such as 1Password, LastPass, BitWarden, or similar, I would advise you to continue using them and deactivate Lockwise features, wherever possible.

Here are a few quick steps to ensure that Lockwise does not cause a conflict with your existing password management software.

Click Privacy & Security in the sidebar and, under the section titled Logins and Passwords , uncheck all the checkboxes, viz.

Ask to save logins and passwords for websites

Use a master password

You might also want to separately uncheck the box that says Show alerts about passwords for breached websites . This is a feature allows Lockwise to anonymously track existing breaches, compare your passwords against them, and inform you if any of your passwords have been 'cracked'. 1Password also provides something similar called Watchtower in conjunction with Troy Hunt's Have I Been Pwned service – same as the one used by Lockwise.

Click the Saved Logins button and evaluate the usernames and passwords if already stored by Lockwise.

[QR Code: https://www.youtube.com/watch?v=DocbhfRMrLo]

These contactless cards issued by banks are based on the NFC protocol, which is how the man in the video is able to charge someone else's card by simply tapping it against their pocket. For a drive-by to be successful, the distance between the two NFC devices needs to be as small as 4-6 cm, which is difficult but certainly not impossible to achieve.

In the next section, which is simply named History , uncheck the box next to Remember to Search and Form History . This will ensure that no form of data gets saved by the browser.

While Firefox Lockwise seems like a useful password management tool, I cannot whole-heartedly recommend it at the moment, since it hasn't undergone the test of time, that is, it hasn't been used by enough users yet. You might want to keep an eye on how things develop over at the companion website, that is, https://privacy.clinic -- scan the QR code given alongside this paragraph and bookmark the page that it opens in your browser.

[QR Code: https://privacy.clinic]

Safari, by Apple

Due to Apple's strong stance on the privacy of user data, Safari does not send any telemetry data back to Apple servers, or provide any syncing and/or personalization options. However, there are a few other settings in your Safari installation that you might want to tweak.

Assuming you are using Safari on macOS, go to Safari | Preferences and follow all of the recommendations listed below:

Default search engines: Choose the Search tab and in the dropdown next to Search Engine , choose a more privacy-aware search engine, such as DuckDuckGo.

Search suggestions: In the Search tab, under the Search Engine dropdown, uncheck the box that says Include search engine suggestions .

Privacy and cookies: In the Privacy tab, check both the checkboxes, under Website tracking , that is,

Prevent cross-site tracking

Ask websites not to track me

Websites: In the Websites tab, you'll find a bunch of options in the sidebar, such as Reader, Content Blockers, Auto-Play, Camera, Microphone, Location, Notifications , and many more. These options correspond to how Safari behaves when it encounters one of these elements on a website visited by you. The default behavior for each of these options can be changed using the corresponding dropdown on the right-hand side.

Autofill: In the Autofill tab, uncheck all four options, that is,

Using information from my contacts

Usernames and passwords

Credit cards

Other forms

Google Chrome

Please refer to the INTERMEDIATE -level recommendations, described further in this chapter.

RohitRecommends

Ordinarily, I would outline each one of the different types of networks and specifically describe mitigation and prevent techniques to ensure that your networks were protected from the various attacks described in the chapter so far.

However, a large part of staying safe on networks involves following some basic hygiene, which I have discussed in this section. There are very few specific recommendations I can give to secure each of the network devices and protocols separately. I'll try and enumerate them separately in this section, wherever possible.

The recommendations in this section have been designed to take into account all possible issues, vulnerabilities largely, and attack vectors discussed in this chapter. While some issues discussed in the chapter require specific intervention, most of the issues can be resolved by following the instructions given under various recommendation levels below.

Extensions

The extensions that I will be recommending in this section are recommended not just by us but by almost all the privacy and security experts around the world. You can always find the latest set of recommended extensions at https://privacy.clinic/

uBlock Origin [5] : uBlock Origin is a completely open-source extension that touts itself as an efficient wide-spectrum-blocker, that is, it goes above and beyond blocking ads. uBlock Origin uses filter lists constructed and maintained by volunteers to identify and block ads from loading on pages. It is available for both desktop and mobile versions of most major browsers. uBlock Origin consumes very little memory and barely interferes in your internet browsing, except for removing any ads or tracking scripts from the webpage that is being loaded.

Privacy Badger: Privacy Badger is an open-source extension that works along the same lines as uBlock Origin, that is, it stops advertisers and third-party trackers from tracking you across multiple websites without your permission. Created by the Electronic Frontier Foundation, Privacy Badger stops third-party trackers but allows first-party tracking in order to promote a balanced approach to internet privacy between consumers and content providers. It employs a heuristic that only blocks advertisers and tracking cookies that do not respect the Do Not Track setting in a user's web browser.

Info

The ethics of ad-blocking

Sometimes, you might hear an argument about how blocking ads is illegal because it stops content producers from earning money for their content. The emotional appeal of the argument certainly makes people think twice before installing ad blockers. However, there are four much bigger, much more important arguments in favor of ad-blockers:

Malware: Since the early days of the internet, ads have often been used to deploy malware on to unsuspecting users.

Aggressive user profiling: In more recent times, advertising networks aggressively collected tons of user data through the usage of 3rd party cookies, to the point where ads began to feel creepily stalker-ish.

Autoplay ads: Even now, inspite of adblockers gaining rapid popularity, websites and advertisers insist on pushing autoplaying video ads which consume not only unnecessary screen space but also consume costly internet data.

Bloated webpages: The stark difference in page sizes and page load times for most websites with and without ads makes adblocking not just a

lucrative option, but a necessary one.

Advertisers and advertising networks have abused consumer trust to a point where ad-blocking is no longer an ethical question but a financial one. In other words, I no longer have any questions about the ethics of using adblockers - I firmly stand in favor of them.

HTTPS everywhere

While most websites have now completely switched over to HTTPS and offer secure browsing for all their webpages, some of them might still use insecure elements on a few pages - wither on purpose, or by accident. The HTTPS Everywhere extension forces the website to use a secure connection (that is, HTTPS) to display all elements on a webpage, thereby ensuring that your browsing experience is made more secure.

BASIC: (1 point)

Staying safe on the internet is mostly based on common sense. Think of it as visiting a large city in an unknown country. As long as you stick to the popular spots and don't venture into shady alleys, you should be safe. All the common sense you would apply in such a situation is exactly the kind of common sense you need to apply on your networks as well:

Safe browsing habits: While 'safe browsing habits' is certainly a broad concept, I have discussed a lot of them in the various #RohitRecommends sections sprinkled across the book. These habits won't come naturally to most people -- in fact, you'll need to follow them in the beginning consciously, but once you get used to it, it'll become second nature to you!

Antivirus andfirewalls: Regardless of which device you use, it is advisable to have a decent antivirus and a firewall deployed on your system. Most operating systems these days even provide their own home-baked solutions. The default Windows Defender software that comes pre-installed on all Windows 7, 8.1, and 10 systems is a pretty good antivirus and firewall solution. On Unix-based systems such as macOS and Linux, firewalls are slightly more complicated than just flipping a switch.

Switch off radios and sensors when not in use: When you're not using them, turn off your Wi-Fi, mobile data, Bluetooth, NFC, GPS, and any other wireless network that you might have left switched on. One, it will help you conserve your battery life and keep your phone alive for longer during the day. Two, if a specific radio isn't broadcasting; the chances that someone hijacks your device go down drastically!

Specifically, check your Bluetooth settings and ensure that your phone is not in Discoverable mode by default! Furthermore, if you use NFC-enabled contactless cards, encase them in RFID-safe covers to prevent your card from being used in drive-by attacks like the one mentioned above.

Do NOT connect to ANY unsecured networks or devices: It is tempting to connect to something that has the word free in its name - hey, who doesn't want to save a few bucks, right? But, the free Wi-Fi may be a rogue AP waiting to MitM your browsing and steal your credentials.

Even if the free Wi-Fi is offered by a person you trust, do not succumb to the temptation. Instead, help them enhance their security by teaching them how to secure their Wi-Fi by setting up WPA2 authentication with PSK (Pre-Shared Key) on their wireless router.

Essentially, it is better to use your own mobile data rather than connecting to an unknown, unsecured network.

Do not accept, download, or open any files from any unknown devices or persons: Often, all it takes to install a backdoor on your system is opening a random file with unknown origins. We saw earlier, in the Android chapter, that malware can be installed on your phone by simply opening a PNG file! Similarly, there exists software that can hijack your device by sending seemingly innocuous files through your Bluetooth connection. Until recently, there existed vulnerability in Airdrop (on iOS and macOS) that allowed an attacker to silently install a malicious app by simply sending a file to an unsuspecting victim.

INTERMEDIATE: (10 points)

Browser recommendation: Same as the recommendations in the BASIC level/section

Private browsing: Same as the recommendations in the BASIC level/section

Privacy settings: I personally believe using Google Chrome is actually detrimental to the privacy of your data. If you insist on using Google Chrome, there are several additional tweaks that you must perform in GoogleChrome settings. That's why I've placed the list of corresponding tweaks to Google Chrome settings under the INTERMEDIATE level of recommendations.

For Google Chrome users, go to Menu | Settings or chrome:\settings and follow all of the recommendations listed below:

Opt-out of telemetry and collection of usage data: In the section titled Sync and Google Services . In the options that are displayed, toggle the following settings off:

Help Improve Chrome Security

Help improve Chrome's features and performance

You may toggle other settings on or off, depending on the level of privacy desired. I recommend leaving Safe Browsing as it prevents you from accessing known malicious sites on the web.

Turn off syncing and personalization: In the section titled Sync and Google Services , toggle the setting titled Do searches and browsing better to OFF . Next, scroll down, open the Advanced Settings , and toggle the Allow Chrome sign-in setting to OFF .

Change your default search engines: In the section titled Search Engine and use the dropdown box to select a different search engine -- I recommend choosing DuckDuckGo instead of Google. If you wish to add a different search engine, simply visit the site or search the internet to find instructions on how to add it.

Search suggestions: In the section titled Sync and Google Services, toggle the setting titled Autocomplete searches and URLs to OFF .

Cookies, tracking, and content blocking: Scroll down to the bottom and click on Advanced to open/unhide the advanced settings. In the section titled Privacy and Security scroll down to Site Settings and click to open it. Under the section titled Permissions , click on Cookies . Among the options displayed underneath, toggle the following settings ON:

Keep local data only until you quit your browser

Block third-party cookies

Ideally, it makes sense to toggle the setting titled Allow sites to save and read cookie data (recommended) to the OFF position, but cookies form an important part of the browsing experience, so I won't recommend turning it off.

Permissions and site-settings: Scroll down and click on Advanced to reveal the hidden settings. In the section titled Privacy and Security , scroll down and open Site Settings . Under the section titled Permissions , you'll find a bunch of options relating to access permissions for the features outlined in the paragraph above. I also recommend toggling all the settings (other than Cookies and JavaScript) to either Ask before accessing or Blocked .

Form autofill: Scroll down to the section titled Autofill and click to open it. You'll find three sections -- Passwords, Payment methods, Addresses.

In the Passwords section, and toggle both the Offer to save passwords and the Auto Sign-in settings to the OFF position. Evaluate and delete any passwords that have already been saved -- both locally and in your Google account -- by performing the appropriate actions in the Saved Passwords section, as and where necessary.

Open the Payment methods section and toggle the Save and fill payment methods setting to the OFF position. Evaluate and delete any payment methods that have already been saved -- both locally and in your Google account -- by performing the appropriate actions in the Payment methods section, as and where necessary.

Open the Addresses and more section and toggle the Save and fill addresses setting to the OFF position. Evaluate and delete any addresses that have already been saved by performing the appropriate actions in the Addresses section, as and where necessary.

Extensions: If all you do on your browser is check your email, share on social networks, and read articles on various websites, then the extensions I am about to recommend are probably not for you. Sure, they might help you with some aspects of your browsing but if you don't know (or can't understand) what the extension does, just skip to the next chapter, directly.

Cookie Auto Delete: The cookies stored by various websites remain on your system until well after you have closed your browser tabs and windows. This is done primarily to ensure trivial conveniences such as not needing to log in the next time you open your browser window. However, it also means that the website that sent you the cookie gets to acquire more information about you and your browsing behaviors. Cookie AutoDelete automatically deletes cookies when you close the tab. Without the cookies, the website cannot recognize you and, therefore, won't be able to create a cumulative profile based on your browsing habits.

Decentraleyes: To save time and bandwidth, websites serve all of their JS/CSS libraries from blazing fast servers called CDNs, or Content Delivery Networks. However, every request made to a CDN server carries quite a bit of information about both, the browser making the request AND the website for which the request was made. CDNs are, therefore, in a unique position to carry out comprehensive user-tracking. The Decentraleyes extension, instead, intercepts the request to the CDNs and serves the requested library from local storage, thereby reducing the possibility of any such tracking by the CDN itself.

Info

Content Delivery Networks

All webpages are primarily comprised of three different kinds of resources -- text, scripts, and objects. Typically, websites rely on JavaScript and CSS to look pretty and perform different actions/animations/functions within the browser itself. There exist several compilations of JS scripts and CSS stylesheets (libraries) that provide lots of different functionalities out-of-the-box. The most commonly used JS and/or CSS libraries are made available through a bunch of fast servers called CDNs , a.k.a. Content Delivery Networks.

Terms of Service; Didn't Read: It is believed that I have read and agree with the Terms & Conditions is the biggest lie on the web -- we often think of it as just another box that needs to be checked to be able to move to the next step. However, this simple action can (and often does) mean signing away significant portions of rights over your own data and your own content. To counter this, a bunch of good samaritans over the internet banded together to create the Terms of Service; Didn't Read (short: ToS;DR) project in 2012. The ToS;DR website (and the ToS;DR add-on, available for most popular browsers) gives short, human-readable summaries of a website's ToS and also grades this ToS on the basis of their impact on the privacy of your data.

INTERMEDIATE: (2 points.)

At this level, I'd ask you to follow all the instructions given under the BASIC recommendation level and also implement the following additional recommendations:

Update the firmware on all devices on a regular basis: A firmware is simply an operating system specific to a device that allows the device to perform specific functions. In that sense, Windows is a firmware for your desktop or laptop; Android OS is a firmware for your Android device; iOS/macOS is the firmware for your Apple device, and so on. Every manufacturer releases updates to firmware whenever serious vulnerabilities are found. Always ensure that you check for firmware updates for all your devices regularly and install any security updates immediately.

Invest in a good antivirus and firewall: There are good antivirus options available that are both free and paid. If you are willing to invest some money, consider purchasing a license for a good antivirus and firewall. A lot of internet security software development companies will offer a bundled product at reduced prices. You might even get a good deal if you purchase them during the Cyber Monday sale or similar.

Some popular options for antivirus and firewalls are mentioned below

Antivirus: BitDefender and Trend Micro

Firewalls : ZoneAlarm and Comodo

Please note that these are not the only recommended options; these are merely the most popular ones. You may choose to opt for a different antivirus and firewall if you so choose.

Monitor your network: To understand what is wrong with your network, you need to have a good idea of how it behaves when it is right. Monitoring your network on a regular basis will give you a baseline definition of what normal and regular look like, on your network. Any deviation from these baseline values should be investigated and acted upon quickly. For example, if your Netflix appears grainy too often, it could mean some application is hogging a majority of your network bandwidth. Or, if your antivirus suddenly refuses to update to the latest virus definitions, no matter how much you try, it could mean that your system has been infected by malware.

Switch to a secure DNS: In recent years, multiple cloud DNS services operated by major players such as Google, IBM, OpenDNS, Cloudflare, and many more, have become available promising greater security, faster resolution, and increased privacy. Some of these services also provide additional features, such as secure communication, ad-blocking, and parental control.

The catch is that your DNS queries are sent to these servers, who can then utilize this data in whatever way they choose. Although most of them claim that they do not store any logs of the DNS queries, there is usually a 24-hour wait time before the logs are deleted. Regardless, I'd still strongly recommend switching to one of these DNS servers.

Among the many options available today, Cloud flare's 1.1.1.1, Quad9 (9.9.9.9) by IBM, and Google's 8.8.8.8 are options you might want to consider seriously. Those looking for ad-blocking might want to look at the Blokade or AdGuard apps, while Comodo SecureDNS (8.26.56.26), and OpenDNS Home (208.67.222.123) both offer parental control options as a (usually free) service for registered users.

ADVANCED: (15 points)

ADVANCED: (3 points.)

The following recommendations require you to invest both time AND money into securing their networks, that is, more for organizations than individuals. However, if your home contains a lot of IoT devices, you might want to follow them too:

Intrusion Detection and Prevention Systems (IDPS): There exist options for detecting and preventing all kinds of vulnerability exploits and unauthorized access on your network. These tools are commonly referred to as IDSs (Intrusion Detection Systems) and IPS (Intrusion Prevention System) - depending on the extent of threat-mitigation they provide. These systems monitor the network for any malicious traffic, log relevant traffic

information, and (may also) take necessary steps to stop them.

IDPS are available in both hardware and software variants, with both open-source and proprietary options available in the software variant. The hardware variants usually market themselves as Next-Generation Firewall, or Smart Internet Security devices or Hardware Firewalls and are usually designed to be plug and play. The modern versions of these intrusion detection and prevention systems are relatively easy to set up and get running.

Some of the popular intrusion detection softwareare:

Snort (Free and open-source, for Windows and Linux)

OSSEC (Free and open-source, for Windows, macOS, and Linux)

Suricata (Free and open-source, for Windows, macOS, and Linux)

As for hardware firewalls/smart internet security devices, you might want to consider:

Trend Micro Home Network Security

Bitdefender BOX

BullGuard Dojo Smart Internet Security and Privacy Solution

Bear in mind though, these devices are somewhat expensive and are recommended only if you absolutely need to secure your internet browsing. For most home-use cases, using these may be unnecessary and rather extravagant.

Virtual Private Networks (VPN): I've mentioned VPNs in quite a few places throughout this book. A VPN is essentially your network connecting to another network, which then connects to the internet on your behalf. This secondary network, which provides a promise of privacy and anonymity, is called a VPN . VPNs are extremely useful in situations where you suspect (or know) that your network traffic is being monitored by an external agency and you want to bypass their spying eyes.

Note

VPNs differ from proxies because they do much more than hiding/spoofing your IP address. A determined attacker will still be able to snoop on your internet traffic (even if it is proxied) and infer the destination website using a variety of sophisticated techniques.

There are both free and paid VPNs that you can use to connect to the internet, although most free VPNs offer severely limited value by either throttling speeds, or restricting data usage. In some cases, using a free VPN may even cause a privacy nightmare for your due to their policy of sharing your browsing data with third-parties.

While there are several free VPN services that offer good-to-decent value, opting for a paid VPN service will most likely result in a better quality of service. Some important aspects to consider while evaluating a VPN service are:

Privacy and logging policy: Look for VPNs who can offer complete virtual privacy to their customers, that is, they do not store any logs or snoop on any of the data being transmitted through their servers, and ensure complete anonymity for its customers.

Security features: Some important security features to look out for, in a VPN, are kill-switches, encryption of all traffic, and the VPN's track-record on security.

Server locations: A VPN that has its servers in privacy-aware locations such as the EU definitely rates higher than a VPN with servers in places with a poor track-record of user privacy, such as the US, UK, and Australia. The geography of the servers also matters in terms of legal jurisdiction, censorship, and surveillance. Plus, having access to servers in multiple countries allows you to access geo-restricted content, too.

Bandwidth, speed, and throttling: Most paid VPNs offer unlimited speeds with a decently-sized data cap. Most free VPNs will throttle either the data or the speeds or both after a predefined limit. In some cases, VPNs may choose to show ads in exchange for offering you free VPN services.

Device compatibility: You can always set up a VPN directly on your device, but most VPN providers provide a separate app for your device. Ensure that the VPN provides an application compatible with all your devices and that ititself is secure and not privacy-averse.

Cost vs value: This is arguably the most important aspect to consider while choosing a VPN. While the basic-tier of most VPNs are priced more or less similarly, the differences in the features offered may result in price variations in premium-tiers that may put a certain service(s) beyond your budget.

Keeping all of these aspects in mind, I would recommend the following VPN services as worthy of consideration for a paid subscription:

ProtonVPN

ExpressVPN

NordVPN

Mullvad

The Tor browser: Another layer of privacy can be added to your internet browsingby using the Tor network instead of (or alongside) your VPN provider. Similar to layers of an onion, Tor adds a strong layer of privacy to your browsing by bouncing your communications around a distributed network of relays run by volunteers all around the world.

Here's what Wikipedia has to say about the Tor project:

"Tor is free and open-source software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router". Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays."

Scan the QR code given alongside the above paragraph to open the Wikipedia entry for Tor in a browser tab on your device.

[QR Code: https://en.wikipedia.org/wiki/Tor*(anonymity*network)]

To extend an analogy I've previously used in this chapter, using Tor is similar to playing Chinese Whispers with the seller in a bazaar BUT without any loss of information.

Using the Tor browser is quite easy. Download the file from the official website (i.e. torproject.org) and run the executable file. Follow the instructions shown during the install process. When the installation completes, simply launch the Tor browser by double-clicking the shortcut named Start Tor Browser in the folder where it was installed.

Browser recommendation

There are three things I would specifically recommend for advanced users:

Use Firefox. Uninstall all the other browsers.

Use Firefox's private windows for any and all casual surfing.

Use the Tor browser for all your private and/or anonymous actions.

Do not mix any of the above three use-cases EVER.

Private browsing

See recommendation above.

EXPERT: (5 points)

As always, the recommendations under this section must be made under thesupervision of someone who knows these concepts thoroughly. Ensure that you have ample backups before you begin and have a sure-fire way of rolling back any changes that you make from this point onwards.

I take no responsibility if anything goes wrong in your attempt to execute the following recommendations:

DNS over HTTPS/TLS: The DNS over HTTPS (DoH) standard was proposed in October 2018, and it involves querying DNS servers over secure, encrypted channels to ensure maximum privacy by preventing eavesdropping and manipulation of DNS data. The DNS over TLS security protocol is already available and implemented by multiple DNS providers (such as Cloudflare, Google, and Quad9) to ensure user privacy and security.

If you are using Firefox version 62.0 or greater, you can enable DNS over HTTPS as follows:

Type about:config in the URL bar and press Enter.

You'll see a warning. Read it carefully, uncheck the box, and press the button that says, I Accept!

In the input field at the top, type network.try and wait for the rows to get filtered. Look for the row titled network.trr.mode and double-click it.

In the dialog box that pops up, change the value from 0 to 2 , and click OK .

Next, look for the row titled, network.trr.uri, double-click on it, and change it to one of the following DNS over HTTPS providers, listed at this URL: https://github.com/curl/curl/wiki/DNS-over-HTTPS

Finally, search for network.trr.bootstrapAddress , double-click on it, and change it to the IP address of the DNS query server, for example, 1.1.1.1 , if you chose Cloudflare in the previous step.

Scan the QR code given alongside this paragraph to open a blog-post titled Configure DNS Over HTTPS in Firefox on ghacks.net, where steps described above have been documented with additional details and screenshots

Privacy settings

One of the quickest ways to create a robust set of privacy-aware settings for Firefox is a service called Firefox Profilemaker . It is made by a GitHub user named allo- and can be accessed at ffprofile.com . The website takes you through a bunch of questions that will evaluate your privacy requirements and generate a Firefox profile specific to your needs. The site also provides detailed instructions [6] on how to 'install' this profile, at the end of the process.

[QR Code: https://www.ghacks.net/2018/04/02/configure-dns-over-https-in-firefox/]

Bespoke NIDS with Raspberry Pi: You can set up a bespoke Network Intrusion Detection System and Firewall using a Raspberry Pi, which will perform the following functions on your network:

Enforce network traffic policies.

Ensure that abnormal packets do not get out or in our network.

DHCP server to distribute network parameters to your LAN.

DNS cache/server to speed up DNS requests and filter out bad DNS queries.

NIDS to detect malicious traffic, such as malware or vulnerability exploits.

Act as a central network monitoring node to watch and debug network traffic.

This method is highly technical and requires significant expertise inthe subject matter, and I would not recommend doing it without expert supervision. If you'd still like to give it a try all by yourself, please look up relevant articles on pfsense, Pi-Wall, and pi-hole to understand the intricacies of setting up a bespoke NIDS and firewall using Raspberry Pi. The QR code given alongside this paragraph points to an article on the Instructables website, which will help you get started with this process.

If you decide to replace your existing Firefox profile, I strongly recommend that you first back up the existing profile folder before you proceed with the steps detailed by ffprofile.com . Scan the QR code given alongside to open the Firefox Profilemaker on your device.

[QR Code: https://ffprofile.com]

[QR Code: https://www.instructables.com/id/Raspberry-Pi-Firewall-and-Intrusion-Detection-Syst/]

Extensions

uMatrix: uMatrix is an extension for advanced users, which provides a point-and-click blocker philosophy and interface (almost like a firewall) for each webpage you browse. According to the developer, uMatrix puts you in full control of where your browser is allowed to connect, what type of data it is allowed to download, and what it is allowed to execute.

Upon installation, uMatrix works in a block-all, allow exceptionally mode, that is, it blocks all 3rd-party scripts from being loaded in the browser. This is likely to break quite a few web-pages, so make sure you know what you are doing.

Firefox multi-account containers extension: Recently, Firefox included a unique feature called multi-account containers to its browser. Multi-account containers allow you to separate your personal, work, shopping, etc. identities without having to log out each time. Each container has separate access to a different part of the browser's storage, which means that all your site-specific preferences, cookies, and tracking data (if any) are associated with the container, rather than the entire browser.

Multi-account containers are a simple and quick method to login (and stay logged in) to several accounts at once without any account interfering with any of the others. This is useful if you created different accounts for your work and personal needs.

Facebook container: The Facebook container is a highly-specialized version of multi-account container that isolates all links related to Facebook (and associated websites such as Instagram, Messenger, and many more) in a separate container. If a website opened in another container happens to include an element from Facebook (for example, the like button), the element itself is invoked in the Facebook container due to the strict policy of the extension.

Thus, any and all cookies set by Facebook (and associated websites) are isolated and your regular browsing stays untracked .

Conclusion

We've looked at privacy concerns with devices, and we've looked at privacy concerns with services on the internet. However, the most important aspect that goes ignored while considering connections between devices and services is the layer that makes it possible, viz. the network. We often don't give much thought to * how * a device connects to the internet, only that it is able to.

Networks are simultaneously the weakest and the strongest aspects of communicating over the internet. We use different kinds of networks on a daily basis, often without properly considering how secure these networks truly are. We assume that our communication over these networks is non-leaky and that our messages reach the desired destination without any interference.

I hope this chapter has opened your eyes to the possibility that these assumptions may not always hold true, especially in the case of unknown networks.

Just like you shouldn't trust an unknown computer, you shouldn't trust an unknown network either. I get it - free Wi-Fi is tempting. Random files sent by anonymous people over Bluetooth are tempting, but you need to overcome that temptation to prevent the possibility of your device getting infected, or worse, breached.

And, if you absolutely must connect to an unknown network, ensure that you have the right security software set up and properly configured on your device. If you can't avoid it, you need to make sure that you are adequately equipped to prevent it from damaging you and your data.

In simple words, prevention is better than cure, and it pays to be always prepared.

---

[1] MAC-spoofing and IP-spoofing both have legitimate uses in software testing, identity masking, and anonymization.

[2] A popular wireless attack tool called ‘Café Latte’ used this technique to recover cached 128-bit WEP keys, and demonstrated the same at ToorCon 9 in 2007

EXPERT: (25 points)

At this level [7] , you probably want to avoid all other browsers and just use the Tor browser inconjunction with software and services that promise similar or better levels of privacy and anonymity, such as the .onion network, Tor-compatible VPNs, anonymous file-drop services, and so on.

Important!!

I do not recommend using this for casual internet browsing at all! Reserve your Tor browser usage for when something serious is at stake.

While Tor traffic is known to be highly secure, extremely anonymous, and difficult to decrypt, it certainly is closely monitored by several entities -- state and non-state actors.

Chapter 13

Operational Security (OPSEC)

Installing Tor

Download the Tor Browser Bundle, and extract it to a folder of your choice. Double-click the icon named Start Tor Browser and wait for it to establish the relay. A short while later, the Tor browser window will open and you will see the standard Tor connection message. That's it, you're done! You can now access any website on the internet with the highest level of privacy and under maximum anonymity.

Introduction

OPSEC (short for OPerational SECurity) is a military term to describe the process of ensuring that casual exchange of information between two friendly members of a unit does not accidentally yield critical information to a non-friendly actor.

As we've seen in the chapters so far, tiny bits of data can be put together to form a larger picture. We have seen how the entire targeted advertising industry relies on this methodology to automagically create profiles for users browsing the internet. Each website visited, each bit of content posted, each video viewed, each product bought -- everything you do on the internet is used to assign a data-point to your profile. A collection of data points big enough can then be used to make a deterministic evaluation about you.

This is where OPSEC comes in handy.

Broadly speaking, OPSEC is a set of processes and behaviors aimed at ensuring that mission-critical information does not get accidentally shared with an adversary. Wikipedia defines OPSEC as follows:

Operations security (OPSEC) is a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.

[QR Code: https://en.wikipedia.org/wiki/Operations_security]

Using Tor

There are a few things to keep in mind while using Tor:

Use the Tor browser as-is -- do NOT change anything!: Although the Tor browser is basically a modified version of the Firefox browser, it is designed and constructed with specific settings to confound browser fingerprinting techniques, thereby ensuring maximum anonymity. If you change any settings, you are likely to change the fingerprint generated by your Tor browser, which could potentially unmask your presence. In simple words:

1) Do not install or remove any extensions

2) Do not change any settings

3) Do not even maximize the window, or change the size/shape of the window in any way, shape, or form.

Do not log in to any websites while using Tor: Although most popular websites on the internet now recognize Tor relays and make adequate provisions, there is always the chance that the automated spam filter might flag you as a bot or, worse, a malicious actor and lock you out of your account. Moreover, logging into an account means identifying yourself to a website with a username and password combination, which basically defeats the whole purpose of using Tor to become anonymous!

Choose Tor-friendly, privacy-aware services in conjunction with the Tor browser: I've already mentioned how Windows does not have a great track record in terms of privacy and security of the end user. If your Windows login is somehow compromised, there is every possibility that your Tor browsing may also end up being compromised. Hence, I strongly recommend that you use Tor in conjunction with a privacy-aware OS such as Tails or Whonix, whenever possible.

The same argument also applies to your browsing habits, incidentally. Most websites attempt to track you and generate a unique profile ID by default. They will then track you across the web using this profile ID and associate every action you take with this profile ID. While Tor tries to ensure that no cookies can be associated with your real identity, there are chances that you may slip up and reveal you're true identity somewhere. Choose privacy-aware options to your usual websites, for example, DuckDuckGo instead of Google, Protonmail instead of Gmail, Signal instead of WhatsApp, and many more.

Use Tor liberally, but carefully and responsibly: Tor works under the assumption that if everyone appears the same to an observer, then no one has a unique identity, therefore everyone is anonymous. This is why Tor attempts to create a uniform identity for everyone who uses Tor. Thus,

every time you use Tor, you add another faceless identity to the crowd which can be extremely helpful for someone who needs it, for example, people trying to communicate in oppressive regimes, or whistle-blowers trying to get the message out.

As a matter of fact, that is also exactly what I have tried to teach you throughout this book. Actions that you don't particularly think twice about can be used by various adversaries against you. Therefore, in the #RohitRecommends sections at the end of each chapter, I've attempted to change either the settings of the system or change your habits. If you followed my recommendations, there is a good chance that you were able to restrict the different kinds of information that your devicesmight have shared with the internet otherwise.

In this chapter specifically, I'll enumerate and explain some of more rigorous processes and behaviors and help you devise a sufficiently secure OPSEC strategy to ensure maximum privacy of your personal data.

Caveat Emp-tor!

[8]

While the Tor browser is a quick-and-easy option for surfing the internet anonymously, one must remember that it works on the principle of building multiple relays between your browser and the remote server. That means your traffic could very well be intercepted by an adversary. (See the section on Tor Browsers earlier in the chapter for a slightly more detailed explanation.).

Although all Tor traffic is encrypted, there is always a possibility that a dedicated adversary could find ways to compromise your system, your anonymity, and expose your identity. Or simply, there may arise certain situations where you require a higher grade of anonymity and privacy than what Tor has to offer. For instance, you may be a celebrity wishing to maintain anonymity in the digital world. Or you may be someone who needs to fly under the radar for reasons involving harassment, bullying, or something similar. There is a multitude of reasons why you might need such a customized solution.

In such situations, I recommend a customized approach, tailored to your specific needs, to maintaining your privacy, the details of which are rather complicated to explain in this guide. I recommend you consult with experts on how best to achieve this for your specific case. You can also refer to the companion website, that is, https://www.privacy.clinic , where you can find detailed articles and casestudies, published from time-to-time, describing how I was able to achieve better anonymity by customizing solutions for our clients in specific scenarios.

An adversarial approach

In terms of OPSEC, it is safe to assume that any person who receives your data or is in a position to receive it may be an adversary. This adversary may be known, hidden, or unknown . For instance, in terms of browsing the internet, you can define known, hidden, and unknown adversaries as follows:

Known: For example, the remote server that hosts the website you are browsing.

Hidden: For example, the cookie placed by an advertiser that collects information about your browsing.

Unknown: For example, an eavesdropper on your network sniffing all your interactions with the website.

Under OPSEC conditions, you always assume that all three kinds of adversaries can track every action you perform. You must also assume that adversaries will collect several actions and piece together a larger picture by analyzing these actions within the appropriate context.

For example, imagine you work with the military, and you urgently need to call someone, but your phone has just died. You could wait, or look for a phone charger, or search for a public phone, or request a stranger to lend you their phone. One of these actions is highly recommended, and one of them is absolutely not recommended. Can you guess which is which?

I'll save you the suspense. Waiting is the highly recommended action and requesting a stranger for their phone is absolutely not recommended.

Remember what I said about adversaries? Well, the stranger is an adversary in this scenario. The simple action of using a stranger's phone revealsat least two pieces of information to the stranger – the number you call, and your physical location to the adversary. A determined adversary could even read between the lines and extract other useful meta-information from the scenario.

Conclusion

In my personal opinion, Google (and its parent company Alphabet) cannot be completely trusted to be privacy-focused. Their entire business

model revolves around finding the right customers for the right advertisers and vice-versa.

That would be like asking a wolf to guard the sheep, wouldn't it?

And I do not voice these concerns lightly; Google has given us several reasons over the years to be distrustful of them. For example, in 2018, Chrome introduced a feature that caused users signed into any Google service to be automatically signed in to their Chrome browser as well. Google insisted (and continues to insist) that this doesn't change any existing data-collection policies, but given how extensive and exhaustive their existing data-collection policies already are, I'm not sure how much of a difference this assurance actually makes.

If all that has got you wondering, which of the popular browsers available today qualifies as privacy-focused, prepare to be somewhat disappointed.

Although both Mozilla Firefox and Safari claim that they are considerate of your privacy, they are privacy-aware rather than privacy-focused, at best. Brave is still a relatively new (and therefore unknown) entity, in spite of all its brave words. Using Tor to access your email and social networks is comparable to using a hammer for etching your name on a grain of rice.

Then there are the other questions:

Does tweaking your browser settings provide enough cover to protect the privacy of your personal data?

Won't the websites you visit continue to store your data long after you close your browser window?

Can you control what these websites choose to do with your data?

And exactly that's what we'll be discussing in the subsequent chapters -- services and networks. Get ready!

---

[1] You'd be surprised by the amount of resistance it can generate if you ask people to switch to a different browser - even if the only change involved requires clicking a different-looking icon.

[2] I would have recommended StartPage but in the time it took me to finish the manuscript for this book, System1 invested in StartPage through one of their subsidiaries called Privacy One. System1 is an advertising company.

[3] Personally, I prefer Mozilla Firefox. I'm not yet entirely clear about Brave's intentions…

[4] Don't worry, if something goes wrong, you can always start with a fresh browser 'profile'.

[5] uBlock Origin and uBlock are DIFFERENT extensions. uBlock Origin was forked from uBlock by the original developer because of shady practices by the maintainer. Make sure you install "uBlock Origin", and NOT "uBlock".

[6] If you decide to replace your existing Firefox profile, I strongly recommend that you first back up the existing profile folder before you proceed with the steps detailed by ffprofile.com.

[7] I do not recommend using this for casual internet browsing at all! Reserve your Tor browser usage for when something serious is at stake. While Tor traffic cannot be easily decrypted, it certainly is closely monitored by several entities -- state and non-state actors.

[8] That's Latin for "Buyer beware!"

The OPSEC process

It is believed that the US military developed OPSEC during the Vietnam War. They developeda protocol to institute processes to prevent mission-critical information from being accidentally inferred by the adversary by piecing together unrelated bits of information.

The project was initially named Purple Dragon but was eventually replaced by the term operations security that was coined to describe these processes during the Vietnam War.

Chapter 10

Services - Email

Scan the QR code given alongside this paragraph to download a PDF of the de-classified issue of Cryptologic Quarterly , and check the section titled, Observations on the Evolution of OPSEC (Operations Security) on page 8.

Also, here's another, telling excerpt from the same report:

The Vietnam War was the catalyst for the development of OPSEC. This war dramatically illustrated the need for OPSEC because the enemy had so much foreknowledge of American activities.

[QR Code: https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-quarterly/remembering*the*lessons.pdf]

The OPSEC process is iterative (that is, to be repeated until all mission-critical information is secured) consists of 5 important steps, as described below:

Identify critical information: You must first establish the information that needs to be protected and understand the reasons why it needs to be protected.

Analyze threats: Next, you must identify potential adversaries, their motivations, and any harmful actions they may execute.

Analyze vulnerabilities: Next, you must analyze your own setup and identify if any potential weaknesses exist that the adversary can exploit.

Assess risks: This step involves exploring the possibility that the adversary manages to exploit the weakness and the fallout of the action.

Apply countermeasures: Now that you have all the necessary information, what can you do to protect your critical information?

While OPSEC's origins may be rooted in the military, this doesn't mean that OPSEC is meant only for military personnel. OPSEC is a behavioral protocol that can be practiced by anyone and everyone. In fact, OPSEC practices come in very handy even in the context of something as banal and mundane as posting a photo taken in your bedroom to social media.

Let's break down this example and evaluate it in OPSEC terms.

Every photo contains embedded EXIF data, which contains highly sensitive information such as the make and model of the device, location coordinates of the place where the photo was taken, and more. To protect this critical information, we need first toanalyze the threats that may affect this critical information.

There are several threats that might arise from this action, but the most immediately identifiable threat is someone (a home invader, a jilted lover, and more) who might be trying to find out where you live. Uploading the photo also renders you vulnerable, since the adversary can use the EXIF data to identify the precise location of your home, thanks to the embedded GPS coordinates. A simple solution to protect your sensitive data would be to use a tool to strip off all the EXIF data from the photo before uploading it to social media!

By answering five simple questions, we were able to identify a useful OPSEC process for action as banal and mundane as uploading a photo to social media. Using these techniques, I have devised a set of instructions in the form of Dos and Don'ts for certain crucial aspects of data privacy in daily life.

In the sections that follow, I'm going to outline these Dos and Don'ts to ensure that your data remains private and secure.

Introduction

Whenever someone says they did something on the internet, for example, bought a dress, posted a comment or an update, uploaded a photo, checked out a website, what do they actually mean? How actually does doing something on the internet work?

Broadly, the process of 'doing something on the internet' can be divided into three parts:

Using an internet-capable device, such as a laptop or a smartphone.

Connecting via an internet service provider, or ISP.

Accessing a service (that is, using a website) over the internet connection.

When you think about it, each one of these three parts contains information relevant (and maybe, critical) to you and your identity. Your device stores information about you. Your ISP provides the infrastructure that carries the information you send to remote servers. The services you access receive (and often, store) the information you send for processing and analysis. Also, each of these three parts, if intercepted by someone, can cause your information to be leaked.

That's why it is important to secure each of these three parts as much as possible.

In the previous chapter, we have already discussed ensuring that the first part, that is, your devices are secured, in quite a bit of detail. I'll be dedicating this section to ensuring that we do the same for the other two. I'll start by looking at some of the most frequently used services on the internet and how to go about securing them, such that they leak as little information about you as is possible. Specifically, I'll be talking about your email, social networks, shopping, banking, and general online behaviors and how to make them secure.

Dos and Dont's

You know by now that OPSEC is a rather detailed investigative process, which involves identifying critical information, vulnerabilities, threat actors, and implementing countermeasures.

That said, there are a few DOs and DON'Ts that I can definitely recommend. I can state with one hundred percent certainty that these will inevitably form a part of the recommendations generated by any (and every) OPSEC evaluation.

You'll recognize some of the DOs and DON'Ts as instructions that you may already be following from earlier in the book. You can still use this section as a reminder to ensure that the settings haven't changed and everything is as it should be.

Mobile phone subscription

Not all banking apps provide the ability to use an authenticator app to generate the OTP for conducting transactions. In most cases, banks prefer to verify transactions by sending OTPs through text messages or verification calls to the customer. On a smartphone, this means that the OTP can be read by a third-party app that has access to your messages -- clearly, a security risk that cannot be ignored.

With that in mind, the following recommendations could help ensure better security for your financial transactions:

Buy a separate phone connection [1] for different usage purposes. For example, use a non-smart phone for all your banking needs and conduct all transactions using the SMS-based or phone call-based OTP, wherever possible.

Use a basic phone (a.k.a. a dumbphone) for your banking needs. One, no one is likely to suspect the significance of this action. Two, you won't be able to compromise the security if you can't install any apps.

Keep the associated phone number private and exclusive for the corresponding usage needs. Use the banking phone for banking calls, the work phone for work calls, the personal phone for personal calls. Use a dual SIM phone to avoid carrying multiple handsets, if required.

If you decide to use a separate phone for your banking and financial transactions, ensure that the phone number stays as private as possible but also use it regularly to ensure that it doesn't get compromised in a SIM-swap attack.

Email

The email was one of the first services to be introduced on the internet, and it still constitutes a major portion of the daily traffic on the web. In fact, according to a recent report by Radicati, there are over 3.9 billion email users worldwide, and they send around 293 billion emails per day. That's a little under one hundred emails sent per user on average.

Device security

Setting up a lock-screen for your device a simple but often-ignored recommendation. The flimsy excuses used by most people for not having a secure lock on the phone, usually range from takes too much time to unlock to forget often the password to what if there is an emergency.

Here's my recommendation: if your device does not have a secure locking mechanism, set it up immediately! Like, stop reading and set it up NOW!

Use the following set of instructions to decide what kind of lock-screen you want on your device:

In terms of security and encryption, a password is more secure than a PIN, and a PIN is more secure than a pattern.

The longer the password, the more difficult it becomes to crack the encryption

Avoid using biometric IDs such as fingerprints, face, and more, to lock, if possible.

If you ever need to decide between using the browser or installing an app to access something, always choose the browser over the app. The browser provides greater control over what personal information is transmitted as compared to an app.

The fewer the apps on your phone, the fewer the vulnerabilities, and the fewer the chances that your phone gets attacked with an exploit.

Ensure that your device has the necessary anti-malware and anti-virus capabilities installed and active on your phone.

In the chapter on smartphones, I have provided a list of recommended apps – ensure that those apps are downloaded and installed on your

phone.

To sum it up in simple words: Set up a lock with a difficult-to-guess password on your phone, avoid using biometric IDs, and use good security software.

[QR Code: https://www.radicati.com/wp/wp-content/uploads/2019/04/Email-Market-2019-2023-Executive-Summary.pdf]

One could make the argument that, due to the growth of instant messaging solutions, the total number of email users is likely to have decreased somewhat over the years. However, email definitely continues to be one of the preferred modes of communication, especially among corporate users.

Emails also constitute a valid form of identity over the internet with a large number of websites choosing to let users supply their email ids as logins, instead of creating separate usernames.

New signups

The internet sees new services being introduced every day, in the form of websites and apps. Sometimes, these apps are interesting enough to warrant signing up on them. However, every new account you create increases the likelihood that your personal data may get compromised.

One way to combat this is to ensure that you do not share any personal data when you sign up to a new service on the internet. There are several ways to make this happen, and we have discussed quite a few of them in the earlier chapters. Here are a few more recommendations along the same lines:

Use disposable email addresses to sign up for websites you are unlikely to visit again. Mailinator, 10minutemail, and SpamGourmet are my preferred websites of choice for disposable email addresses.

Ensure that you have complete knowledge of which services automatically shares your information on a public profile.

Use non-identifiable, anonymous usernames and emails like cooldude33 or moonlight44, while signing up.

Avoid giving out your personal email address. Instead, use separate email accounts for each sign up. You could use a mail-forwarding service like boun.cr and 33mail.

Use a strong password, a password manager, and Multi-Factor Authentication (MFA) using a good authenticator app rather than SMS.

Consider using an offline password manager instead of an online password manager. Use separate databases with separate passphrases to store passwords in the contextthat is, Personal passwords in the personal database, Work passwords in the Work database, and more.

It is important not to lose track of the various accounts that get created over time. I would recommend that you execute a clearing-up of inactive accounts at regular intervals of time, say every six months or so. You can even make it coincide with your semi-annual password changing routine, to make it easier to remember.

These are merely a few examples of the various scenarios where you might need to consider adopting OPSEC practices. In truth, there are tons of situations where using OPSEC would be absolutely necessary. There is more than enough content to fill an entire book on the subject, but we'll have to make do with just a small chapter for now.

I'll say just this: OPSEC is a philosophy, not an end goal. Like all philosophies, it requires you to ask a lot of questions and search for answers. Like all philosophies, it teaches you a certain way of life. Like all philosophies, it may give you answers you may not like to hear.

And, like all philosophies, it is entirely up to you how strictly you want to adhere to it.

Accessing email

There are two distinct people access to email in one of two ways:

Online: By logging in to the email web portal in your browser.

Offline: By logging in through an application (for example, an email client) on your device.

As is obvious, each method has its own pros and cons and its own set of dos and don'ts, which I'll outline one-by-one in the #RohitRecommends section of this chapter.

Conclusion

Throughout this book, in each of the chapters you have read so far, I've given you various recommendations on how to prevent your personal information from being accessed without your consent. I've provided processes and methods of varying levels of difficulty (ranging from BASIC to EXPERT) to combat the unnecessary sharing of data by various devices, services, and the networks that connect them.

Cultivating OPSEC behavior in your day-to-day life essentially involves adopting all of those recommendations and making it into a habit. It involves extensively evaluating the results of each action and finding a suitable option that ensures little to no leakage of critical information.

To put it simply, adopting OPSEC in your life requires extreme awareness of your actions. It requires you to consider each action carefully and evaluate the potential ramifications of the action and then devising counter-measures which will ensure minimal fallout.

Just to give you an example, consider the simple, mundane action of checking your email. Ordinarily, you'd open a browser window, enter the website address, and log in to your account. OPSEC requires that you evaluate each one of these steps, identify threats and vulnerabilities and find counter-measures that protect your personal information. In all likelihood, in this scenario, you'd end up using your TAILS bootable USB or a Whonix gateway to open up Tor browser on a trusted network to log in to your email inbox with a password manager and MFA enabled. It might seem excessive, but that is what OPSEC is all about -- lots of caution and very little left to chance.

Of course, OPSEC scenarios may not make sense in day-to-day proceedings, where maximum privacy is not really required. However, having OPSEC knowledge helps in the same way it helps to know how to change a tire. You don't need to do it every day but, in the rare case that your tyre gets punctured on a highway and leaves you stranded, you should know how to do it yourself.

I mean, you can't always rely on the possibility that a Good Samaritan is going to appear out of nowhere to come and help, can you?

---

[1] You cannot buy a mobile connection without proper documentation (e.g. Know Your Customer, or KYC) in many countries. Buying it in someone else's name is absolutely NOT recommended!

Web-based portals

The practice of storing emails locally using an email client has clear and major privacy implications. Specifically, it violates the first guiding principle of privacy mentioned in the very first chapter. In this regard, web-based portals score over email clients due to their on-demand nature, that is, they only display email that you request.

Web-based portals are preferred by people who need to access their emails from different devices at different times. Although email apps on the smartphone have replaced browsers for this specific need, there may still be instances where logging into your account using a browser may be preferred.

Chapter 14

Epilogue

Email clients

Email clients work slightly differently from web-based portals in that they require you to provide your access credentials only once -- usually during setup.

Once the email server authenticates the login credentials and authorizes the client, the client downloads emails from the server at regular interval using the login credentials already supplied. These emails are stored locally on the device, as opposed to retrieving them from a remote server on demand, in the case of web-based portals.

Compromising your email

The process of compromising an email account is a lot simpler than it seems but a lot more difficult than most people are led tobelieve. Unlike the myths made popular by several movies and TV series, malicious actors do not spend their time trying to figure out passwords letter-by-letter.

Instead, they use a variety of different techniques to infiltrate your email account and/or your device then and access crucial data from within. I'll outline some of the most common methods used by malicious actors so that you are aware of what to expect. Later, in the #RohitRecommends section, I will provide concrete steps on how to prevent and/or mitigate these threats and ensure that your email account stays as secure and private as possible.

Introduction

You have now reached the end of the book. Congratulations!

If you made it this far AND also followed my recommendations along the way - well done!

Let's take a quick look at how your efforts have shaped up, shall we? Here's the same QR code that you scanned in the first chapter. Bring out your smartphone, scan it (again) and open the link that appears on the screen.

Phishing

The technique of impersonating a friendly contact to elicit sensitive information from a target/victim is called phishing and it is a common method used by attackers to compromise email accounts. It works like this:

An attacker crafts and sends a fake email with language and content designed to look like it could have been written by someone you know. The subject line is usually something simple and generic like, Read this and tell me what you think. or You'll love watching this!

When you click the link to the attachment, a webpage opens up requiring you to log in to your email account to read/view/listen to the attachment. This webpage is always fake and can be identified as fake by looking at the URL in the address bar. For instance, instead of saying google.com, it might say google.com or google.com.update.securesite.app.site –note that neither of these is the official Google website address.

[QR Code: https://leaktest.privacy.clinic]

If someone (for example, johnsmith@gmail.com) actually enters their credentials on the fake webpage, their credentials are captured, and the victim is redirected to the actual login page for their email, leaving them none the wiser.

Do the results look any different from what you saw the first time?

Using the credentials acquired in the previous step, the attacker takes over the inbox of the victim (johnsmith@gmail.com) and sends out mass emails to everyone in the address book. With the same content and fake attachment used in step 1.

If you did follow my recommendations, they should. If you never went beyond the BASIC recommendations, you are unlikely to see much change in your results, since the BASIC recommendations were mostly about providing you with relevant information and equipping you with knowledge.

This time, however, the email has legitimacy since it is sent using johnsmith@gmail.com's email account. The percentage of people who will click the link and enter their login credentials is likely to be higher, resulting in the attacker being able to capture even more credentials.

Of course, I am not saying you must follow only the EXPERT recommendations -- it wouldn't be a very smart thing to do, and it is guaranteed to throw your daily routines completely off-track!

I mean, can you imagine living your life without Google Maps? Or even Windows 10, in some cases? Sure, there are several alternatives for those services, but I don't want you to adopt those alternatives just because I tell you to -- certainly not at the cost of making your life difficult [1] . I want you to make an informed choice based on the information presented to you in this book.

Throughout this book, I have attempted to show you how these services might leak your private information. I have tried to teach you the different ways to stop that from happening, or alternatives if you can't stop that from happening. It is entirely up to you to make an informed decision about what works best for you from a cost-benefit analysis perspective.

Anyway, let's analyze your scores and try to understand how exactly (and how much) following all those recommendations haveimpacted your privacy.

Weak passwords

Numerous internet security firms have examined and analyzed the millions of passwords leaked in various data breaches. Almost all of them agree that the most common password used by people is: 123456 . The second most common password is usually either password or 123456789 .

We often overestimate our ability to make up good passwords. We often tell ourselves that coming up with secure passwords is easy. In fact, some websites on the internet also claim to provide useful techniques to generate secure-yet-memorable passwords, such as:

Sentence abbreviation: I know what you did last summer!! can be written as !kWyDL5!! which is a somewhat strong password.

The XKCD technique: First suggested by popular comic xkcd.com, it involves combining four common unrelated words such as CorrectHorseBatteryStaple to form one secure password.

Mnemonic devices: For each account, imagine an unlikely scenario and make a mnemonic device, for example, for your Gmail, think of a Shark riding a Pineapple on NH7, and combine them to create GmSh4rN3aPnh7!

Language-mixing: This only works for non-English languages that use an alphabet/script different than the Roman alphabet. Writing native words in the Roman alphabet/script (for example, 2Aankhen12Haath?!) can qualify as a pretty secure password under most circumstances.

Note

If you haven't seen it yet, scan the QR code given alongside to open the specific XKCD comic that first suggested/presented the technique.

Interestingly, the specific password given as an example in the XKCD technique (that is, CorrectHorseBatteryStaple) is not so secure anymore and has already been cracked, according to the Have I Been Pwned database. I definitely do NOT recommend using CorrectHorseBatteryStaple as a password for any of your accounts!

Updated analysis

If you have been keeping a score of the various recommendations you followed through the book, now is the time to tally all of them and get a final score.

If you scored:

0 - 50 points, then you are a “Novice.”

51 - 100 points, then you are an “Amateur.”

101 - 150 points, then you are a “Pro.”

151 - 200 points, then you are a “Legend.”

What do these titles mean?

The Novice: You probably earned this title because you chose to follow mostly the BASIC recommendations. Now, there's nothing wrong in that, but this basically tells me that you either like keeping yourself informed or you are afraid to take the next step [2] .

[QR code: https://www.xkcd.com/936/]

Well, now would be a good time to revisit all those recommendations and take the next step, I guess. You already have the information, why not act on it?

The Amateur: You didn't want to risk following any of the ADVANCED recommendations, correct? You essentially stopped yourself from attempting the ADVANCED recommendations because you were afraid you might end up accidentally breaking something. Well, you won't know until you try, will you?

Malware

An attacker with access to your email account can craft specific emails (see the additional information box for Phishing) that are designed to infect your system with specific malware, by sending them disguised as harmless attachments.

Many victims have believed outright lies such as, Oh, don't worry, go ahead and click 'Install' on that attachment. I assure you it is completely harmless! simply because the attacker replied from the compromised email account.

Once the victim installs the malware, the attacker gains access to a lot more than just the email accounts. For example, the attacker may install a keylogger that makes it possible for the attacker to intercept *everything* you type, or view, or download, or install - pretty much everything you do on your system.

Thankfully, most antivirus and antimalware software are advanced enough to detect these kinds of intrusions but requires scanning your attachments for virus and malware before you open them.

Look, I'm not saying you should go back and break something. I'm saying if you don't break it, how will you learn how to fix it?

The Pro: Ah, the intrepid explorer! You like tweaking things and changing things, and getting your hands dirty, don't you? You like pulling out the guts and examining them closely to see if they reveal any secrets, don't you? I bet your favorite part of watching crime shows is when the forensic analyst comes on screen!

Email ads

We've now gotten so used to seeing ads in our email inbox that we don't even stop to consider for a moment how they got there. More often than not, these ads seem to be precisely targeted, highly relevant to our immediate needs. The pin-point accuracy of such ads raises the question, "Is someone reading my emails?"

Sadly, the answer is, Yes .

Your email service provider can 'read' your emails, in the sense that they can process the content of your emails, extract the relevant keywords, identify products that correspond to those keywords, and serve ads for these products directly into your inbox. If you use a web-based portal, these ads may appear as banners, or contextual links, or a specially positioned email, or any other variety of sponsored listing . If you use an offline client, these may take on the appearance of a regular email mixed between your other emails.

Every email service provider who offers free email services scans all your emails and harvests them for useful keywords. The only way you can prevent your private emails from being read is either:

Hosting your own email server

Using a privacy-aware email service provider

Let's take a look at both of these options in a little more detail.

I'm just kidding. It is good to see you make an attempt to actively try and change the status quo instituted by Big Tech. I'm proud of you, carry on!

The Legend: Hey there! Glad to make your acquaintance! I hope you liked this book. Do let me know your honest thoughts -- my contact details are floating somewhere on the internet. If you do find them, give me a call on the first Saturday of any month, between 5 PM and 6 PM. I'd like to involve you in my next project.

Hosting your own email server

This option requires substantial and expert knowledge of email technologies. You will have to ensure that:

You own and maintain your own domain and mail-server.

Your domain and mail-server are always white-listed.

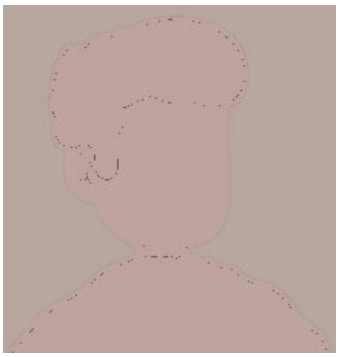
Your server is always secure.

Your inbox is free of spam.

Emails coming to (or sent from) your mail-server don't bounce.

The software running the email server is maintained and up-to-date.

…among many other things. Clearly, this option gives you complete control over your own data but requires you to be completely hands-on.



Something tells me you are going to love it. ;-)

Using a privacy-aware email service provider

Let's be honest; option one might not be everyone's cup of tea. That's why option two, that is, using a privacy-aware email service provider, is probably a better option for those who wish to ensure the privacy of their data but aren't looking to invest too much of their time and other resources into maintaining their own email server.

There are several email providers who provide privately-hosted email services. Some of them provide a free account, but most of them offer paid plans. Some of them even offer end-to-end encryption, i.e. emails sent from your inbox are encrypted before they are sent and, therefore, can only be decrypted by the intended recipient.

Some of the most popular examples in this category are ProtonMail, Fastmail, Hushmail, and many more. While Google claims that they do not scan the emails for personalized advertising, they do scan your emails to provide you other related services such as relevant search, integrations with other Google services, providing intelligent features.

Conclusion

Imagine, for a moment, the life of Harry Truman, the unwitting star in the fictional universe of The Truman Show . His life was a carefully constructed series of events in which he had no active role to play but which definitely played an important part in his development. Everyone around Harry was in on the secret, but no one was allowed to tell him. His life was a carefully constructed facade, beamed live to millions of viewers, while he continued to exist in blissful ignorance.

If you were in Harry Truman's shoes, would such a life be truly representative of the real you? If most of your decisions were a result of choices that were severely limited, were the decisions truly decisions in the first place? Would they even be valid?

The reason I am talking about The Truman Show is thatit is a surprisingly good analogy to what we've been discussing through this book.

You are Harry Truman in this scenario. The domed studio shown in the movie is the internet. The people around Harry Truman are the companies tracking your information on the internet. Their behaviors are the ads that you see on the internet and Harry's likes and dislikes determine whether the behaviors reappear or disappear from his life.

For a large part of the movie, Harry does not get to make a 'real' decision about any part of his life. He merely gets to choose from a severely limited set of options presented to him as fait accompli.

Don't you think the whole thing is a pretty good metaphor for the internet and privacy on the internet?

That's also why I decided to write this book. I believe your personal data should be afforded the same rights as your body -- no one should be allowed to take advantage of it, certainly not without your consent, and the consequences of violating your trust should be severe.

Sadly, the people who were supposed to ensure that our personal rights did not get violated did not pay much heed to things as they were developing. It has now reached a point where privacy on the internet is (mostly) a myth. In fact, any discussions about the right to privacy on the internet are summarily dismissed either as pipe-dreams or as a hipster rebellion . It is sad that this current state of affairs has become the new normal.

Privacy is not a pipe-dream; it is a fundamental right. It is high time we decided to have a coherent and mature discussion around the subject. I am glad you chose to join me in having this discussion. Now, I urge you to have this discussion with someone else.

I'll leave you with these words from the movie, The Laundromat:

Privacy and secrecy are two different things. Privacy is locking the bathroom door when you want to take a pee. Secrecy, on the other hand, is locking the door because what you are doing in a bathroom is not what people usually do.

What we do behind closed doors should be nobody else's business anyway, no?

---

[1] No matter how much Windows disrespects the privacy of your personal data, using Linux is sometimes just NOT an option, you know? *cough* gaming *cough*

[2] There is also a distinct possibility that you were selective in scoring the points or that you didn’t score yourself in some chapters.

Spam

Ongoing research by Valimail indicates that at least 3.4 billion fake emails are sent every day. Another research puts the number for spam email much higher -- at 14.5 billion emails per day. In other words, spam contributes to about 45% of all email traffic.

Chapter 15

Bonus Chapter: Useful Tips and Tricks

[QR code: https://www.valimail.com/press/more-than-3-billion-fake-emails-are-sent-worldwide-every-day-valimail-report-finds/]

Identifying and isolating spam emails is an important task that needs to be performed regularly to ensure that you do not get overwhelmed by it.

However, this is easier said than done. The popularity of email as a login identity means that several websites and services across the internet are in possession of your email and will use this information to send unsolicited promotional material to your email inbox. Therefore, it becomes incredibly important to identify and isolate spam before it floods your inbox.

Don't get me wrong; spam by itself does not pose a threat to your privacy or security of your email account. However, an inbox flooded with spam becomes pretty much unusable if the spam continues to pile up. Legitimate emails may get drowned in spam and may cause loss of valuable business and income.

In 2012, it was estimated that spam cost businesses about $20.5 billion per year – a number that was expected to grow to $257 billion per year by 2018.

That's why I always insist that you should have a separate email address to signup for all the unimportant stuff. There are also several other options that you can use to ensure the privacy and security of your inbox, which I will discuss shortly in the relevant section of #RohitRecommends .

The 10 Android permissions listed under “dangerous” protection level.

At the time of writing this book, there were 10 permission groups classified under the dangerous protection level that could be toggled on/off for various apps.

In this appendix, I've listed the category of apps that typically use these permissions and apps that *atypically* use them. Atypical usage refers to usage that is not immediately intuitive. For example, some banking apps and shopping apps will often request SMS permission to read OTP messages from the SMS inbox directly.

In this appendix, I’ve also presented potential risk profiles for each permission and described the hypothetical scenario(s) in which these permissions may be misused.

Body sensors: This permission allows an application to access data from sensors that the user uses to measure what is happening inside his/her body, such as heart rate.

Typical usage: Fitness apps, companion apps for fitness wearables.

Atypical usage: Calorie counting apps.

Risks: Information about your health can be shared with malicious apps, which might share/sell it to other malicious third-parties.

Calendar: This permission group allows an application to read and write the user's calendar data, that is, create/update and display calendar entries made by the user.

Typical usage: Calendar apps, meeting apps, and more.

Atypical usage : Banking apps, email apps, GTD apps, and more.

Risks: A malicious app can share the details of your personal calendar with third-parties which may include people interested in your whereabouts.

Call logs: This permission group allows an application to read and write to the user's call log, that is, create/update, and display calls made and received made by the user.

Typical usage: Dialer apps, launcher apps.

Atypical usage: Apps like TrueCaller use this permission to provide 'global' caller identification services.

Risks: Malicious apps can upload your call history to their servers and sell it to other malicious third-parties.

Camera: This permission allows an application to access the camera device.

Typical usage: Camera apps, photo apps, social networking apps, scanner apps, and more.

Atypical usage: Banking apps, shopping apps, MFA apps, browsers, and more.

Risks: Malicious apps having access to your camera could secretly turn it on and record your activities.

Contacts: This permission allows an application to read and write to your contact list, that is, create/update and display contacts stored in your phonebook, on your device. It also allows applications to access the list of accounts (for example, WhatsApp, Facebook, Instagram, Twitter, and more.) used on your device.

Typical usage: Dialer apps, social networking apps, email apps, and more.

Atypical usage: Calendar apps, shopping apps, ride-sharing apps, messenger apps, banking apps, and more.

Risks: Malicious apps with access to your contacts can share/sell your address book data with other malicious third-parties who can then use the data to spam, phish, scam, or do any number of similar illegal activities.

Location: This permission group allows an application to access approximate and/or precise location, that is, identify where you are based on the cellular networks in your area or by using the GPS sensor to identify your exact location.

Typical usage: Maps app, ride-sharing apps, delivery apps, camera apps, and more.

Atypical usage: Companion apps to wearables and IoT-enabled devices, shopping apps, social networking apps, and more.

Risks: Malicious apps can track your location to build a profile of your daily habits and frequently-visited locations. Photos and/or social media updates with geotags embedded in them can be used to identify your home and/or work address. There have been instances of robbers targeting homes of users who have posted on social media about being out on vacations.

Microphone: This permission allows an application to record audio. Typically combined with the camera permission, it allows users to record videos with sound.

Typical usage: Camera apps, music recognition apps, dictation apps, voice assistant apps, and more.

Atypical usage: Speech-to-text apps, home-automation companion apps, keyboard apps, note/memo apps, even WhatsApp and more.

Risks: Apps that respond to keywords are quite popular among people but, for them to work, they need to be listening to ALL the time. This means your audio is constantly recorded and evaluated, and not always at device-level. Sometimes, audio may be sent to remote servers for processing, where there could be potential for malicious actors to intercept private communications.

SMS: This permission group allows an application to read, write, and send SMS text messages, receive WAP push messages, and receive MMS messages

Typical usage: Messaging apps, communication apps, and more.

Atypical usage: Banking apps, shopping apps, ride-sharing apps, and more.

Risks: Some apps request this permission to auto-read OTP messages and save you the trouble of entering it manually. However, malicious apps can use this permission to automatically subscribe you to unwanted paid services, or send messages to premium numbers, or spam people in your contact list.

Storage: This permission is the most commonly requested permission, and it allows an application to read and write to the external storage on your phone. Unlike internal storage, external storage is NOT sandboxed; that is, apps writing to the external storage on your phone can also READ other folders in your external storage. Granting this permission to an app typically implies that you are comfortable with the app accessing the various folders in your external storage.

Typical usage: Most apps

Atypical usage: Most apps

Risks: Apps that have been granted permission to read and write to external storage have the ability to read, change, and delete ANY file in your external storage. A malicious app could easily run specific commands to delete ALL the files in your external storage.

Telephone: This permission allows an application to read the state of the device, that is, the phone number of the device, current network information, the status of ongoing calls, and a list of accounts registered to the device. Apps granted this permission can make/answer/redirect calls, use VoIP, among other things

Typical usage: Dialer apps, launcher apps, call recorder apps, and more.

Atypical usage: Banking apps, shopping apps, messaging apps, and more.

Risks: Malicious apps can spy on your phone calls, track incoming and outgoing numbers, and even make calls to premium numbers without your consent.

How to setup your Android without Google Services

Google Mobile Services, while they may seem tightly-coupled with the Android OS, are not entirely necessary for Android OS to function. There is an entire ecosystem of apps and services designed to allow you to operate an Android phone without requiring Google services.

This, however, requires a fair bit of technical know-how and I recommend that you continue along this path if and only if:

You have experience with installing anOS on computers and phones.

n and password) were to fall in an adversary's hands, how bad would it be?”

99 times out of 100, the answer inevitably is some variation of, Very, VERY bad!

You have either flashed or rooted Android phone (or jailbroken an iPhone) at least ONCE in your life.

We all have things in our email inbox that we don't want the world to see. Any adversary gaining access to your email inbox will probably end up getting access to not only your personal conversations, but also your financial information, your social media accounts, and a bunch of other online identities. Very few people keep a zero-inbox policy and clear everything out of their inboxes.

You have a clear idea of the various ways in which tinkering with your phone can go horribly wrong.

useful to have important emails stored in your inbox. We also have to acknowledge the flip side, though -- as long as those emails remain in your inbox, there is always a possibility that someone might be able to access them, without your knowledge or consent.

You agree that you and YOU alone will be responsible for whatever happens to your device if you follow any suggestions outlined from here on.

Since you are still reading, I will assume that you said yes to all of the conditions above. If not, skip to the next section NOW!!

There are multiple tutorials available on the internet, and I strongly recommend that you search for one that is suitable for your phone model and follow along closely. Due to the speed and frequency of updates to both phone hardware and software, the information that is presented in this book is likely to be at least a little bit obsolete by the time it reaches you. The overall process is likely to be the same, but the specific steps are likely to be different for different phone models at different times.

Having said that, here's what you'll need to do to use Android without any of Google's services:

Identify a suitable custom ROM

Okay, first things first, you will need to figure out if a suitable custom ROM is available for your phone model. Typically, Lineage OS (previously known as CyanogenMod) or some version of AOSP (Android Open Source Project) should be available for your specific phone model. If you don't find your phone model on this list, I strongly recommend that you abort this attempt and head straight to the next section, NOW!!

Prepare your phone

Important!!

WARNING!! Be very, VERY careful of what you do here. This part is a bit tricky, and it could brick your phone, that is, render it into a very expensive paperweight. Consider yourself warned!

You will need to unlock your bootloader and flash a custom recovery on your phone. The steps involved in this process are quite intricate and involve using specific commands to unlock the bootloader. Also, unlocking the bootloader may void the warranty of your device, so please be absolutely sure that you *want* to do this.

Look up your phone model on Google and see if you can find a detailed step-by-step description of the process. Head over to XDA if you can't find your phone model on Google - they may have unofficial ROMs that might be suitable for your phone. Usually, the forum post will also have the corresponding instructions on unlocking your bootloader and flashing a recovery.

Again, if you don't find them even on XDA, I strongly recommend that you abort the process immediately.

Boot into the recovery mode and MAKE A BACKUP!!

This is, without doubt, the MOST important step because flashing a custom ROM requires completely wiping your device. You will lose ALL of your data, and I mean ALL your data -- downloads, Bluetooth transfers, apps you may have installed, settings you have changed, documents, games -- every single thing!

Typically, the most common recovery tools include a backup option that will allow you to, well backup everything on your phone. Alternatively, you could use third-party software such as Titanium Backup Pro, or NANDroid to make a complete backup of your phone in case things don't work out the way you plan.

Remember, however, that these backups are often quite large, so you might need to make space in your phone storage to ensure that the backup goes off without a hitch. This is a necessary step in case something goes wrong while installing the custom ROM and you have to revert to previous settings.

Download MicroG instead of GApps

Most Custom ROMs are AOSP-based and, as a result, they do not include the core Google apps and services. However, many third-party apps rely on the Google Play Services framework to run correctly on Android.

MicroG bridges this gap by providing a pathway to install these necessary services on your device but without the use of Google and their default environment.

For more details, you can refer to the excellent guide on GadgetHack titled, Use Android Without Any Google Apps or Services, found here:

https://android.gadgethacks.com/how-to/use-android-without-any-google-apps-services-0193735/

Accessing your email

For an attacker, it doesn't really matter at all whether the email is on a server or stored on your local machine, as long as they get some kind of access to it. What truly matters in this scenario is creating enough barriers of entry for attackers to delay them just long enough, so that you can reach out to the authorities.

So, how do you create barriers to entry? By simply following good security practices around your email accessing habits - it's as simple as that, really!

Scan the QR code shown alongside to open the link in your browser.

Wipe your System and install the custom ROM

I will refrain from giving any generic instructions in this section because there is no one-size-fits-all when it comes to installing a custom ROM. You'll have to search the internet for a post or a (tutorial) video that deals specifically with installing a custom ROM on your device and follow the instructions to the letter.

In fact, I strongly recommend that you follow the instructions exactly as written/shown to minimize any chances of bricking your phone. Just make sure that you *don't* wipe your internal storage or you will be left without any OS on your phone, that is, you'll end up bricking your phone!

If you did everything right, you should be able to boot your phone into the custom ROM of your choice! Enjoy your shiny new custom ROM!

Web-based portals (BASIC, 1 point)

In case you plan on using a browser to access your email through the web-based portal, the standard set of do's and don'ts is applicable.

Always use the secure site - look for https and/or the lock icon in the browser's address bar.

Login to your email only if you trust both the device and the network.

Use your browser's private browsing mode on devices and networks you aren't familiar with.

Log out of your email account and close the browser window when you are done.

Use strong passwords in conjunction with a password manager, wherever possible.

Always use multi-factor authentication to log in.

Understand the terms of service and privacy policy laid out by your email service provider.

In fact, I recommend choosing browsers over smartphone email apps whenever possible, since apps are far more intrusive and have lesser regard

for the privacy of your data. If you absolutely must use a smartphone app, choose an app (preferably open-source and trusted) that respects your privacy, such as K-9 Mail, Fair Email, or ProtonMail.

Useful apps that you should definitely consider installing

By now, you must have realized that the inherent insecurity of smartphones makes the idea of privacy a difficult one to maintain - especially when it comes to Android phones. Despite the best efforts of manufacturers and the engineers at Android, the availability of millions of apps in the Google Play Store means that the chances of finding malware are much higher than normal.

Therefore, there are certain kinds of apps that, we think, are an absolute must for every smartphone – both Android and iPhone. We'll try and cover as many apps as we can in the subsequent sections. However, this list is neither exclusive nor exhaustive. That is, not all apps that appear on this list are absolutely necessary, and this list does not list ALL the necessary apps. Also, we are not affiliated with any of these apps, but we can certainly vouch for them based on our research and knowledge of the subject.

That said, you can always refer to the latest, most updated list of these apps over at the companion website to this book, that is, privacy.clinic. Scan the QR code given alongside this paragraph to open the relevant page on your phone, right now.

Offline clients (BASIC, 1 point)

As with web-based portals, I have compiled a list of dos and don'ts for accessing your email through email clients:

Lock your email client with a strong password when you aren't accessing it.

Do not share passwords with your co-workers.

Do not download attachments from unknown senders.

Scan attachments for antivirus and malware after downloading them.

Make regular backups of your email to an external device -- online and/or offline.

I cannot stress how important it is that you do NOT leave either your email client or your system unlocked. Anyone with access to your device or system can easily read through any and every email in your inbox!

[QR code links to https://privacy.clinic/privacy-related-apps-for-your-smartphone]

Password managers

What: Password managers take away the hassle of remembering passwords for various sites and services by providing a secure vault to store all your passwords.

Why: Most users regularly reuse their passwords -- a practice I do NOT recommend. If the password you re-use were to get leaked, all of your logins immediately become vulnerable.

How: Using a password manager allows you to set complex passwords without having to remember them – the password manager service does the remembering for you. You can use the built-in random password generator to set an absurdly long password, filled with special characters.

I strongly recommend changing all your passwords to lengths of 20 characters or more wherever possible, as soon as possible.

Popular options: Lastpass, 1Password, Dashlane, and KeePassXC

Authenticators

What: Multifactor authentication (MFA) is an additional layer of security for your devices and services. The most commonly known form of MFA is two-factor authentication, (2FA) which is available with most of the popular services on the internet.

Why: The advantage of having 2FA enabled on your device/service is that, even if your password were to be leaked somehow, an attacker wouldn't be able to gain entry into your device/service without the correct OTP which can only be accessed using one of these apps, or by accessing your text messages or answering the OTP call on your phone.

How: When you turn on 2FA for a device or a service, you need to enter an additional one-time-password (OTP) along with your regular username and password to completely access the service. This OTP can be generated on your device using one of these Authenticator apps called TOTP, or time-based OTP or gets sent to your phone via text message (SMS) or a phone call.

Popular options: Authy, Google Authenticator, and Azure Authenticator.

Ad blockers

What: Ad blockers are a fairly recent addition to the internet, and they do exactly what the name says -- they block (most) ads from appearing on your device screens. Think of it as having a doorman sitting outside your frontdoor, who screens all incoming guests and prevents unwanted guests from entering your house without your explicit permission.

Why: I understand that ads are a way for content creators to make money on the internet. However, many ad networks indulge in pervasive and intrusive tracking of the user, which is something I cannot endorse in good conscience. Moreover, the risk of malware infecting your phone due to misleading ads is also quite high. That's why I strongly recommend using adblockers on your device.

How: Ad-blockers route your internet requests through a locally installed VPN on your device. The requests are then compared against curated lists of known adservers and blocked when a match is found.

Popular options: Blokada and AdAway

VPN

What: VPNs are secure connections to another network over the internet. A securely encrypted VPN also prevents malicious actors from sniffing your internet activity and exposing your private details.

Why: VPNs are extremely useful when it comes to bypassing online censorship imposed by authoritarian governments, evading nosy ISPs, or just generally any entity looking to block your digital experiences. VPNs allow you to access geo-restricted content by bypassing IP-address based filters used by such websites.

How: VPNs change your public-facing IP address to that of the VPN, allowing you some degree of privacy and anonymity.

Popular options: ProtonVPN, Private Internet Access, ExpressVPN, and Nord VPN. Expert users may even want to setup their own VPN server.

Privacy-aware search engines

What: A privacy-aware search engine, much like the default Google app, provides useful search results for your chosen keywords but it respects your privacy by not sending/storing additional meta-data every time you conduct a search.

Why: The default Google app is designed to collect a ton of data and store it on Google's servers. This data is analyzed by Google to provide you with highly personalized suggestions and recommendations. However, research has shown that too much personalization results in users being trapped in a filter bubble; that is, only the information that is palatable to users gets greater visibility.

How: Using a privacy-aware search engine helps circumvent the filter-bubble since your searches and activities are not tracked for personalization. Privacy-aware search engines, therefore, are helpful in making the user aware of multiple options and alternatives.

Popular options: DuckDuckGo, Startpage, Qwant, and more.

Secure instant messaging apps

What: Secure instant messaging apps use end-to-end encryption to ensure that the message being sent can only be read by the intended receiver of the message. If the message were to be intercepted, it would remain unreadable, since the only person with the proper decryption key is the intended receiver.

Why: In 2013, it was revealed that the NSA (National Security Agency, USA) was collecting hundreds of millions email and instant messaging contacts directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple. Soon after, in 2014, the Electronic Frontier Foundation (https://eff.org) released their instant messenger security scorecard, which gave a perfect score to only 7 out of 39 messaging apps available at the time.

How: Secure instant messaging apps employ end-to-end encryption, that is, the message gets encrypted on your device with a key that is only available with the intended recipient.

Popular options: Signal, Wire, Telegram, and Wickr.

Private browsers

What: Private browsers are browsers designed to keep your personal information safe by utilizing highly-secure end-to-end encryption.

Why: The default Browser app on your Android smartphone or the Google Chrome browser can be quite intrusive since they are designed to collect tons of data about your browsing habits. I strongly recommend using private browsing, because browsers are meant to share details of the internet with you, and not vice-versa!

How: Judging by the amount of data your browser shares with various third-parties, one could say that modern browsers share more similarities with two-way mirrors than windows. Pairing a good private browser with a good, privacy-aware VPN significantly decreases your identity footprint and may help render you (somewhat) anonymous, too.

Popular options: Firefox Focus, Tor Browser, Brave, Epic, and more.

App locker

What: Most modern phones provide an app locking feature that inserts an additional lock screen before the app is available for you to use. Users must unlock this additional lock-screen before continuing to the app.

Why: If an adversary gains access to your phone, they should not be able to access any of these apps easily. It needs the ability to prevent direct access to any apps that contain sensitive data, such as banking apps, gallery apps, and note-taking apps, password managers, and more.

How: Check if your phone has an in-built app-locking feature by opening Setting and scrolling down to There are third-party apps that perform this function quite securely, and you might want to look into that option as well.

Popular options: AppLock by Norton, Applocker by DoMobile, and more.

Compromising your email

Whether you prefer downloading emails to your client or viewing them on web-based portals in a browser, there is a set of basic rules -- a set of Dos and Don'ts, really -- that is applicable to both methods.

Alternative app stores

Phishing

An App Store, as the name suggests, is a repository where you can search for and download apps for your smartphone. Typically, for iPhone users, this would refer to the App Store and for most Android users; this could refer to the Play Store.

Most email service providers do a good job of scanning for such threats and keeping them from even appearing in your inbox. However, as I described in the corresponding section above, ONE email is all it takes to undo all that hard work.

I say most Android users because, unlike Apple iOS, Android allows for the possibility of using different repositories for sourcing and installing your apps. Apple does not. If you want to sideload even a single app on your iPhone; you'd have to jailbreak it first.

Furthermore, privacy works on the principle of healthy skepticism, that is, even if you trust something, you always look for additional verification. Even if you trust that the email was sent by your friend john.smith@gmail.com , always verify that the email indeed came from john.smith@gmail.com and not john.smith@gmai1.com [1] or some variation thereof.

There are several reasons why you might want to install an alternative app store. Some of the main incentives are:

Moreover, if the email sounds like something John wouldn't usually write, you should always independently [2] verify whether the email was actually sent by john. smith@gmail.com or if his inbox was compromised (that is, Phished) by an attacker. If the latter turns out to be true, the first thing you must do is change the password to your email account. The second thing, help john.smith@gmail.com to change their passwords and send out an email to all contacts in the address book informing of the phishing attempt.

Recommendations and curations: Alternative app stores have their own recommendation engines, which could result in you discovering different apps. Some alternative app stores may also occasionally (or frequently) post curated lists of apps.

Localization: Some alternative app stores are localized to cater to a specific category or people, for example, a specific country.

However, alternative app stores are also fraught with a lot of risks, since their security policies may not be as rigorous as Google and the Android Play Store. There may be a significant risk that your phone might get infected with malware from a shady app in one of these alternative app stores.

BASIC: (1 point)

In simple words:

Always verify BOTH the email and the sender!

The most powerful weapons against attempts to gain unauthorized access into your digital properties -- be it email, social networks, online banking, and more. -- are a keen sense of caution and trust your instincts. If you feel something is wrong, then the chances are high that something probably is wrong.

For Android

For example, some phone manufacturers like Xiaomi even have their own App Store, where users can download and install additional manufacturer-branded apps for their smartphones. However, apps from one store are usually not installable/usable on phones made by other manufacturers, but you'll have to check that.

That said, there do exist several full-fledged alternatives to the Google Play Store that provide similar functionality. Some of the notable ones are:

Amazon App Store: Developed by Amazon, it offers close to half a million apps (both free and paid) that you can download and install on your Android device.

F-Droid: A community-run, free software project, F-Droid is developed by a wide range of contributors and only hosts apps that qualify as FOSS (Free and Open-Source Software) .

Samsung Galaxy Apps: Initially developed by Samsung as a collection of companion apps for the Samsung Galaxy series of phones, it was recently opened to all developers.

A quick search on Google will reveal many more app stores catering to different niches; for example, the AppsLib store was designed as a store for tablets but didn't seem to have gained much traction. Aptoide is another independent app store that provides the ability for developers and manufacturers to create their own app stores for their users. There are a bunch of browser-based app-stores as well such as SlideME, GetJar, and more.

One thing to note is that you won't find any of these app stores on Google Play Store. Instead, you'll have to open the web page in a browser, download the installation file (usually a .apk file) if it is available, and install it manually on your Android device.

Passwords and authentication

No matter how secure your passwords look or feel , there is a possibility that you may not be able to remember them. Moreover, there is a limit to the number of email-password combinations that one can remember.

Based on the details discussed so far, here are my recommendations for managing your login credentials and processes.

For Apple

Like I said earlier, Apple does not allow for the installation of apps that aren't downloaded from the official App Store -- not even sideloading. There are a few alternative app stores available for the Apple iPhone. However, these aren't truly independent and app stores, that is, they have basically curated app repositories running with an exclusive enterprise license granted by Apple. You may find good promotions, deals, and discounts on some apps but, overall, the apps they carry are the same as the ones available on the Apple App Store.

You will need to jailbreak your iPhone if you want to truly slideload apps on your iPhone. For jailbroken iPhones, Cydia is the go-to App Store, and it is automatically installed when you jailbreak your iPhone.

You can add multiple source-repositories in Cydia, but be careful, as adding a malicious repository could potentially infect your jailbroken iPhone with malware.

Conclusion

Apple does not allow installing independent alternative app stores and the only way to use one is to jailbreak your iPhone. I've already explained to you in a previous chapter why that may not exactly be a good idea. Jailbreaking an iPhone is not something you should do as a spur-of-the-moment thing. It is a decision that can have serious consequences and needs to be thoroughly vetted with someone knowledgeable about iPhones before it is done.

For Android, the only alternative app store even worth considering is F-Droid , and I suggest that you definitely give it a go. The apps on F-Droid are free and open-source and, as a result, they usually lack the polish typically seen in the apps available on the Android Play Store. However, what they lack in terms of design, they usually (more than) make up in terms of functionality, security, and privacy.

The other app stores mentioned above are also worth considering but, remember, each new app store is a separate attack vector for malicious actors to propagate their malware. Sure, some of them may have exactly the app you are looking for but, before you install the app, make sure you stop and consider both the inherent risks and ethics of your actions at least once, especially if you are looking to pirate the app. Furthermore, there may be apps on these alternate app stores that may contain malicious code. You might end up completely bricking on your phone just because an app promised you an 'easy hack to win all your 2v2 matches in your favorite battle royale game' and you were naïve enough to believe it.

I would strongly recommend that you stick to the default app stores -- better the devil you know and all that.

BASIC: (1 point)

There are two different ways you can prevent attackers from easily gaining access to your account. You can use either one or both of these methods to enhance the security of your account.

Use Multi-Factor Authentication: I've already spoken about multi-factor authentication and using authenticator apps like Google Authenticator, Authy, Microsoft Authenticator, and more in a previous chapter but, to reiterate, here's how Wikipedia defines it:

"Multi-factor authentication (MFA) is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism…"

Almost all of the popular websites on the internet -- email services included -- provide multi-factor authentication mechanisms for their users. However, this is not turned on by default; you need to activate this in your account settings. To activate it, you need to either download a compatible authenticator app or provide a phone number that can receive one-time passwords via text message. You will also be presented with a list of recovery codes (that is, codes you can use in case you lose access to your Authenticator app) that you need to store safely.

Regardless of whether you access email through a web-based portal or through an email client, I strongly recommend turning on multi-factor authentication for your email account. The added layer of security is well worth the extra hassle of entering an additional code while logging in to your account.

Password Management Software: Even if you have Multi-Factor Authentication enabled on your email account, you should change/update your password regularly. This is actually easier if you use any of the various excellent password manager services available on the web. Some of the most popular password managers that you can consider using are LastPass, 1Password, Bitwarden, Dashlane, KeePass, and more.

The most powerful argument in favor of using a password manager is the fact that you can literally set a password as long and as complex as N#ifR^T&*YGbnHY!iuGHboi$o!8nC$r9% and never need to remember it! In fact, most password managers come with secure password generators, i.e. automated tools that create random combinations of letters, numbers, and special characters of the desired length, which can be used as an extremely secure password.

Most importantly, NEVER EVER WRITE YOUR PASSWORD DOWN ANYWHERE!

Malware

One of the most common methods of malware infection is through malicious attachments sent via email. Malicious actors will typically use one of two approaches:

The Spray-And-Pray Approach: In this approach, attackers send malicious attachments in generic emails designed to evoke curiosity in people. Users unknowingly download the file and try to open it, which results in their devices getting infected with malware.

The Targeted Approach: This approach is typically used by active adversaries, who will send specially crafted emails to increase the chances that the attachment is downloaded and executed.

In both approaches, the ultimate goal remains the same -- infecting the target system with malware that can wreak havoc in the various ways described in the previous chapters.

Based on these scenarios, here are my recommendations for preventing (or mitigating) malware infections on your device.

Checking your email on an unknown computer

If you ever need to log into your email on an unknown computer, that is, a computer that is not your home computer or work computer, I recommend that you:

Do NOT log in at all.

DO NOT LOG IN AT ALL!!

However, if you absolutely must log in to an unknown computer, follow these steps to ensure maximum privacy and minimize any potential security issues:

Ensure that you have MFA enabled for your email account.

Choose one of the following options:

1) Use a bootable USB to load a secure, live OS such as Tails or Whonix.

2) Install a VM, Use the removable disc option to load an ISO of a live OS and boot it up.

3) Download and install a sandboxing application such as Sandboxie, BufferZone, or similar.

4) Download a portable and/or sandboxed version of your favourite browser, for example, BitBox.

Install the corresponding browser extension for the password manager you use for your email.

Open the private browsing option for your preferred browser and open your email login webpage.

DO NOT TYPE OUT YOUR PASSWORD UNDER ANY CIRCUMSTANCES!

1) Use the password manager extension to log into your email account!

2) Fill out the OTP shown by the authenticator on your device.

While your email is loading in the browser:

1) Log out of the browser extension for the password manager.

2) Uninstall it. Leaving it installed is a much, MUCH bigger security risk.

Do not download any attachments or files, if possible. Instead, forward them to whoever needs it. If you absolutely must download an attachment, remember where you saved it.

After you are done checking your email, SIGN OUT of your email account.

Close the private browsing window. This ensures that any leftover cookies, data, and many more, get deleted.

Depending on what you did in step 2, perform the corresponding reverse procedure, that is, uninstall the sandbox application, or shutdown the VM, or reboot the live OS.

Or,

You know, if you want to save yourself all this hassle, do NOT log in to your email account on an unknown computer.

Your Privacy Score Card

Total Privacy Score: _____ points

Dated: _____

For more information, go to https://privacy.clinic

BASIC: (1 point)

The simplest way to defeat the malware menace and ensure that your device doesn't get infected is to always scan any and all attachments before downloading and opening them. Most popular email service providers (such as Gmail, Outlook, and many more.) provide cloud-based antivirus services, for example, VirusTotal for Gmail.

Info

VirusTotal and Your Email Attachments

VirusTotal was originally created by Spanish cybersecurity company Hispasec Sistemas, launched in 2004, and subsequently acquired by Google in 2012.

It provides several methods to scan your files, including desktop and mobile apps, browser extensions, and API scripts. Scan the QR code given alongside the paragraph to open the Tools section of the VirusTotal website, which lists the various tools available to scan files and URLs.

[QR code: https://support.virustotal.com/hc/en-us/categories/360000162898-Tools]

INTERMEDIATE: (2 points)

If your email service provider does not scan attachments for malware, you can either:

Scan the attachment using a web-based virus scanner , such as VirusTotal.

Scan the downloaded attachment using the antivirus software on your device .

You might also want to consider switching to an email service provider who can (and does) provide better security for your email inbox.

ADVANCED: (3 points)

If you absolutely must open a file from an unknown sender, use a good sandboxing software (described in the previous chapter) or a virtual machine to test run files from unknown sources. Malicious files typically [3] can't escape the isolated environment of a sandbox (or a virtual machine) thereby ensuring that your primary system remains unaffected.

Only when you are absolutely sure of the files true nature and intentions, should you open it on your primary system.

Email ads

Based on the various factors discussed in the corresponding section above, here are my recommendations for countering the privacy-threat posed by email advertising:

BASIC: (1 point)

Understand what data exists within the mails in your email inbox.

Backup and delete any emails that may contain highly sensitive information such as login credentials, passwords, financial information, and many more.

Also, delete unimportant emails from your inbox. Keep your inbox clean and free of clutter.

INTERMEDIATE: (2 points)

Migrate your family to a paid plan on your existing email service provider to ensure that your emails continue to stay private and free from any prying eyes.

Alternatively, opt for a free (or paid) plan with a privacy-aware email service (such as ProtonMail, Hushmail, Fastmail, and many more.) that provides end-to-end encryption for your emails.

ADVANCED: (3 points)

If you own your own domain, chances are your domain service provider already provides you with a (fairly limited) email service, for a specific number of accounts. Several email service providers allow you to utilize their services for your own domain, for example, emails sent to rohit@privacy.clinic can be read using ProtonMail's email service

Consider using PGP extensively in all your email communications, using reliable external, and third-party tools such as GnuPG if, when, and where necessary. You can utilize these tools to encrypt a portion (or all) of your message and digitally sign it with your private key.

EXPERT: (5 points)

Set up your own email server with end-to-end encryption. There are several tutorials available on the web (and on the companion website privacy.clinic) that will assist you in the process of setting up your own mail-server, complete with open-source spam-filter software.

Be aware that setting up your own private email server requires substantial expertise, not to mention putting in several hours of work to ensure that

everything runs smoothly, with minimum fuss. Furthermore, it can be only made as secure as the technologies of the current day will allow it. That means you need to ensure that your mailserver (and the software running on it) is constantly monitored, and kept updated with the latest versions and/or patches.

Spam

The problem of spam is a bit tricky.

On the one hand, as a business owner, being able to send unsolicited commercial communication is definitely a useful tool to have when you are looking to attract new customers. On the other hand, unsolicited commercial communication (specifically the unsolicited part) could be deemed a significant violation of the enduser's privacy.

As an end-user, however, the classification is absolutely clear: Spam is always unwanted, unwelcome, and the less we get to see of it, the better.

To that end, here are my recommendations for tackling spam emails for your email account.

BASIC: (1 point)

Regularly train your junk filter by diligently marking any spam mail that may have accidentally arrived in your inbox. Conversely, mark any mail that may have accidentally ended up in your Spam folder, as Not Spam to ensure that future legitimate deliveries do not get accidentally categorized as Spam.

If your spam email has an Unsubscribe link or button, use it.

If your spam email seems to be originating from someone you know, try and independently verify with the known party before clicking any link or downloading any attachments from the mail.

INTERMEDIATE: (2 points)

Use filters to automatically segregate and categorize email you cannot unsubscribe from into separate folders. Some filters will also allow you to delete the mail without opening it if you want. Tread carefully as this might result in loss of valuable information.

If your email service provider allows it, generate a different alias for your email for different purposes. For instance, Gmail allows you to create an alias with the + sign, that is, if you address is john.smith@gmail.com , then john.smith+amazon@gmail.com, john.smith+flipkart@gmail.com , and john.smith+anything@gmail.com are all valid addresses. Also, john.smith@gmail.com & johnsmith@gmail.com both are the same address, as are j.ohn.smi.th@gmail.com . The number of periods in your Gmail addresses doesn't matter -- they all get sent to your inbox.

Specific details on how to generate aliases for other email addresses can be found in the Help section of your email service provider's website. Typically, you can visit the Account Settings page of your email service provider and check if they provide the alias feature for your account.

ADVANCED: (3 points)

Use a disposable email address to sign up for accounts that require your email address. Websites like Mailinator and GuerillaMail are a couple of examples of popular disposable email accounts with public inboxes. The inboxes can be accessed without a password, and the contents of the inbox are wiped clean every 10 minutes or so.

Hint

A disposable email combined with a strong password, multi-factor authentication, and saved in a password manager is (arguably) a pretty good example of a well-secured login mechanism. Any attacker attempting to breach this set up will have first to crack the (invariably long) password, and then figure out the OTP from the authenticator app.

Alternatively, you can use an email forwarding service such as 33mail or boun.cr to create a second identity which will receive all preliminary email and then forward it to your primary email account depending on rules you have defined. Several hosted email solutions also provide the ability to use them as an email forwarding service.

EXPERT: (5 points)

If you have hosted your own domain, or if you are using a hosted email service provider, you cancreate a catch-all [4] email address on your mail-server. Catch-all email addresses send all email that does not have a valid recipient to a single master inbox. Thus, if you have a mailserver running on example.com and you give someone the address jane.smith@example.com , which doesn't correspond to a valid account on your server, the mail will get delivered to the default account on example.com

You can use this feature to create specific email addresses to create separate login identities, for example, amazon@example.com or

flipkart@example.com . Essentially, having a catch-all email address is like having a disposable email inbox (such as 33mail or boun.cr) but specifically bound to domain name and mail-server.

Prevention and mitigation

BASIC: (1 point)

If like me, you too believe in the saying, Prevention is better than cure then here is a set of three simple instructions that you must definitely follow while accessing your email account:

Avoid public Wi-Fi

Who doesn't love free Wi-Fi? All of us have connected at least once to one of the free Wi-Fi hotspots available at airports, railway stations, and hotels, haven't we?

Here's the thing, if you didn't enter a password while connecting to the Wi-Fi, you might be at risk for an Evil Twin attack on your device. After successfully executing an Evil Twin attack, an attacker, can intercept and monitor all communication to and from your device, without being detected.

That means, not only your email but your social networks, your online banking, your web browsing - everything you do while connected to the Evil Twin Wi-Fi can be intercepted using a type of attack called MitM -- Man in the Middle.

Ensuring that you only visit secure websites (that is, ensuring that the lock is visible in the address bar) while on public Wi-Fi can mitigate some (but not all) of the risks associated with the Evil Twin attack.

The best solution, however, is to never connect to any unsecured wireless networks . If, for some reason, you do connect to one, make sure that the device ‘forgets' the network and delete it immediately from the device.

ALWAYS SIGN OUT OF YOUR ACCOUNT!!

Let's face it; no one typically uses strong passwords for their lock screens, do they? Most screen passwords can be figured out with a little bit of knowledge about the user and the password hint provided by the OS. Put those two together with some smart deciphering ability and, more often than not, you get the lock-screen password right.

Note

I could have included this particular piece of advice under one of the other sections, but I feel I can't emphasize this enough. I can't even begin to tell you the number of times I've found logged in accounts when reviewing security practices for my clients. Accounts containing important and confidential company data that, if leaked, could cause the company huge losses.

Seriously, I can't stress this enough. Always, ALWAYS sign out of your email account and close the browser before leaving your desk!

If you primarily access email through web-based portals, I strongly recommend logging out of your account and closing the browser at the end of every browsing session - no exceptions. Leaving your account logged in because I'll need to open it again in a few minutes or I'm only going to be away from my system for a short while is not just a bad security practice; it is an open invitation to adversaries to compromise you.

A locked screen is probably the mildest deterrent to the adversary who is determined to compromise you and/or your data.

INTERMEDIATE: (2 points)

Review account activity frequently

Some of the popular email service providers will send an email to your alternate account if they feel like suspicious activity might be happening on your account. These emails may also provide you with immediate options to mitigate the effects of any unauthorized access to your account.

Almost all the major email service providers store detailed access information about your account, that is, they store details about the times, places, browsers, IP addresses, and many more, from where your account has been accessed. This information is usually available for you to review -- usually in the Privacy section of your Account -- under the heading Activity History or Activity Details something similar.

You should review your Activity History regularly to check if your account has been subjected to unauthorized access by checking and comparing the various details under account activity.

A handy list of dos and don'ts

Do not reply to out-of-character emails even if they are sent by friends/acquaintances.

Always verify the name and email address of the sender properly and carefully.

Do not reply to emails sent by random strangers.

Be VERY careful with attachments!

Do not open attachments that make you log in to a website.

Do not use public networks to access any personal or professional email accounts.

Regularly review the Account Activity of your email account.

Never write down your login credentials anywhere.

Encrypt your emails with PGP, whenever and wherever possible.

Bookmark this page for quick access, in case you need a reminder.

Conclusion

Your email address is not just a token for communication -- it is a core part of your identity on the internet.

In fact, most of us often use this same email address to sign up for various websites and services on the internet. There is a significant chance that the email you use to log in to Facebook is the same as the one you use for twitter, Snapchat, Instagram, and many more websites. Usually, the argument for doing this goes along the lines of, Well, I don't have multiple identities in real life, why should I have them online! or I don't have time to remember multiple email and password combinations!

However, by reusing the same email address for all your identities, you are essentially providing both advertisers and adversaries with a complete package of your data under one single identity -- your email address.

What happens if that identity gets compromised? Or worse, what if it entirely ceases to exist? For example, if Google decides to shut down your account, what would happen to all your online identities? What would happen if Google were to shut down the entire Gmail service? They don't *have* to continue providing Gmail as a service, especially as a free service, do they? Would you be able to switch to a different email provider quickly and painlessly?

You have a responsibility to take every effort to ensure that this identity -- this core identity that defines a large part of your existence on the web -- does not get compromised easily.

---

[1] I hope you noticed that the ‘l’ in the email address is actually the number ‘1’.

[2] You could call or send a text, or meet face-to-face, etc. to confirm.

[3] Some advanced malware can used sophisticated techniques to identify sandboxing (or virtual systems) and change its malicious behavior accordingly.

[4] A ‘catch-all’ email address, as the name suggests, is an email address that accepts and receives all incoming email and redirects it to different inboxes depending on the specific identity on the incoming email.

Chapter 11

Software-as-a-Service (SaaS)

Introduction

Email is no longer the only reason people use the internet.

These days, the internet provides various other utilities that have far surpassed email in terms of usage, both retention-wise and frequency-wise. It is not uncommon to see people opening multiple websites in different tabs in the same browser window. We often log in to our email in one tab, check out what our friends are doing on Facebook, or LinkedIn, or Instagram in another tab, browse products on Amazon, or Flipkart, or Myntra in a third tab, conduct some financial transactions in a fourth tab, and so on.

The internet has given birth to a multitude of services, all aimed at replacing some task or the other -- tasks that would take a significantly greater effort in real life. Through social media, we are able to stay in touch with our family, friends, and acquaintances. Email and instant messengers have completely replaced the traditional postal mail in most scenarios. Not many people visit the bank these days -- most banks provide a

netbanking portal for people to carry out a lot of the commonly executed financial transactions. Shopping for something has become a lot easier thanks to multiple e-commerce sites that sell products catering to a wide variety of interests. Even planning holidays has become a lot easier thanks to travelling websites that provide end-to-end services, which you can access by simply logging in on their websites!

These websites that provide specific services over the internet are commonly referred to as SaaS, which stands for Software-as-a-Service. The companies behind these websites design and develop the software but, instead of selling the software as a product that people can purchase and use, they host the software on a central server and provide access to individuals who wish to use the product.

So, what exactly is SaaS?

SaaS is what people usually mean when they say your data is stored in the 'cloud'. Think of SaaS as just another way to describe a specific service that you are accessing over the internet.

For example, imagine you are a student, searching for answers to a highly specific question. In the earlier days, you'd spend all the time looking in the library rifling through various reference books to find a satisfactory answer. Alternatively, if you were looking on the internet, you'd start by opening a somewhat relevant website and depend on reference links to investigate further.

In fact, this is how early search engines operated. Search engines like Altavista, Ask Jeeves, and Lycos, would read through their index of millions of websites on the internet and pop up results when the search query appeared among them. Searching the internet would sometimes take seconds or even minutes, and it was heavily dependent on whether or not you used the 'correct' search term! Google changed the whole search engine game by adopting a different methodology that returned results in several orders of magnitude quicker. Where searches could sometimes take minutes to execute, Google almost always returned results in milliseconds.

Info

As of August 2019, Google still shows the time taken by its servers to perform the search. You can see it in parentheses next to the number of search results.

Most regular searches are performed in less than a second, but if you can craft a somewhat lengthy, vague-ish query, you can make Google work for a couple of seconds. Go ahead, try it!

Now, Google could package this unique search engine technology into installable software and sell it as a product that everyone could install on their PCs. However, indexing and storing millions of webpages requires massive computing power that is not affordable for everyone. So, Google decided to offer their software , that is, their advanced searching technology, as a service to anyone who desired to use it.

In other words, Google chose to host their software on a central server and offered it to all users across the internet, as a service anyone could use by visiting their webpage.

One might argue that the internet was designed to connect us to various people and services across the world, and exactly that is what SaaS ensures. However, by now it must be obvious to you, dear reader, that each new SaaS that you sign up to is a potential attack vector. In fact, each new tab that is opened, each new website that we sign in to, is another avenue for a potential attack on our privacy and our personal data.

Types of SaaS

When you think about it, any websites on the internet that require you to sign up would be classified as a SaaS - email, social networks, netbanking, e-commerce - all of them are software programs that are provided by their developers as a service.

Broadly speaking, all SaaS can be classified into four categories:

Social SaaS

Shopping SaaS

Financial SaaS

Other SaaS

In the sections that follow, we'll be providing a few examples of popular SaaS in each category, what data they expose, how vulnerable they could be, and some ideas on how to secure any accounts you might have on their servers.

Social SaaS

All Social SaaS contribute to one of the largest uses of the internet and can be broadly divided into two categories:

Social networking: Social networking SaaS primarily focus on connecting you to various people and/or businesses that you know and interact with.

Social media: Social media SaaS is designed to collect information from a selection of sources much, much broader than your network and present them to you.

These two capabilities of Social SaaS -- networking and media -- need not necessarily be exclusive. In fact, in some cases, a single SaaS can have both networking and media capabilities embedded in the architecture and design of the SaaS. Facebook, Twitter, Instagram, or LinkedIn are good examples of a combined SaaS.

Other apps may choose to focus on one capability over the other exclusively. For instance, WhatsApp focuses on providing instant messaging between people by connecting them through their existing phone numbers.

The common examples are Facebook, Twitter, Instagram, LinkedIn, WhatsApp, Snapchat, Line, WeChat, Hike, YouTube, Twitch, TikTok, Discord, Reddit, Pinterest, Tumblr, VK, Flickr, Meetup, and many more.

Shopping SaaS

One of the first innovative uses of the internet was the ability to simply log in to an e-commerce website such as Amazon, or eBay and purchase a product you wanted. Over the years, e-commerce has grown from selling just physical products to selling all kinds of products and services - both physical and otherwise. You can buy gifts, hire cars, order food, rent hotels, book vacations -- basically any and all kinds of goods and services at the touch of a button.

In fact, under this category, we include all apps that provide any kind of product OR service in exchange for money. Therefore, along with the standard e-commerce sites like Amazon, Flipkart and eBay, we'll also include cab aggregators, travel and holiday planners, classified ads, delivery services, and many more.

However, this fantastic ability to shop for goods and services online comes at a price - pun unintended.

Every time you buy something on the internet, you are also sharing a bunch of highly private and sensitive details, such as your name, your address, your financial details, and other private details such as the products you are interested in, with the shopping site and its partners. You implicitly trust them to keep all that data secure.

The common examples are Amazon, Flipkart, Myntra, Snapdeal, Ajio, AliExpress, eBay, OLX, Quikr, Swiggy, UberEats, Zomato, UrbanClap, Dunzo, BigBasket, Ola, Uber, Cleartrip, MakeMyTrip, Yatra, and many more.

Financial SaaS

In my honest opinion, one of the biggest advantages of the internet has been the availability of banking and financial services online. Being able to access account details and conduct transactions over the internet have been a blessing in so many ways, hasn't it?

Gone are the days when you needed to visit your bank branch and stand in the queue to transfer money from one account to another. These days, all you need to do is enter a bunch of numbers on your bank's netbanking portal, and the banking SaaS takes care of the rest. Getting your latest account balance doesn't require you to go to the bank and get your passbook updated -- all you need to do is open your banking app and, voila, there it is!

In fact, banks these days even provide their own smartphone apps that let you access a ton of banking and financial services. You can use your bank's official smartphone app to perform various tasks such as accessing your account details, transferring funds, managing various financial instruments such as FDs, PPF accounts, credit cards, and loans.

To ensure the highest level of security in online and smartphone interactions, banks often go the extra mile, much beyond the standard step of implementing a secure communication layer between your browser and the remote server. Most banks implement some extreme security measures in place on their netbanking portals, for example, disallowing common browser behavior (such as, right-clicking, or hitting the back button or the refresh button) or forcing you to change passwords every six months, or making you re-login after an extended period of inactivity. As a matter of fact, if your bank's portal or smartphone app does not have such extreme measures in place, you might want to reconsider your relationship with the bank!

Note

Even if your bank doesn't require it, it is a good idea to change your netbanking passwords every six months. Privacy experts are equally divided between committing the password to memory and using a password manager, so we'll let you decide for yourself. In any case, do not write your banking credentials where they can be seen or accessed by others.

However, banks aren't the only financial SaaS available over the internet. There exist a category called NBFCs (Non-Banking Financial Companies) that provide independent SaaS-based portals and smartphone apps. These are often hybrid apps that are primarily designed to provide easy payment mechanisms and also integrate corollary shopping experiences to incentivize usage of their SaaS.

The common examples are ICICI, HDFC, SBI, IDBI, Pockets, PayZapp, Yono, PayTM, Google Pay, mPesa, Freecharge, MobiKwik, and may more.

Other SaaS

This section encompasses all those SaaS that do not neatly slot into one of the above categories but still run in the cloud . Examples under this category might also fit into multiple categories without falling neatly into either one of them.

For instance, StackOverflow and Quora are SaaS websites that operate a Q&A service, but the user interactions and website design indicate a secondary focus on social networking. Similarly, Slack and Discord are primarily collaborative apps, but they have found use as the modern IRC and Yahoo! Chatroom equivalents. Dropbox, Google Drive, and Box provide document storage services -- something that doesn't fall neatly under any of the categories mentioned above.

Essentially, this category encompasses all services that fulfil ALL three criteria:

Run their operations in the cloud that is, on remote servers.

Provide an interface to access these services over the internet.

Do not qualify neatly under any of the above categories.

The common examples are StackOverflow, Office 365, Dropbox, Google G Suite, Box, WebEx, Zoom, Zapier, JiRA Atlassian, Confluence, Slack, Keybase, Discord, GitHub, and many more.

Privacy and security concerns

I would like to acknowledge here that most popular SaaS websites take security and user privacy very seriously.

However, that doesn't mean they are totally invulnerable. There is no perfectly secure solution that covers all possible adversaries and all kinds of attacks. If it did exist, every website in the world would already be using it. However, it would still leave one aspect of the service vulnerable - the user themselves.

Due to its very nature, all SaaS directly violates the first two guiding principles of privacy:

No local data storage -- retain no information locally about the user and their activities.

No remote data storage -- do not sync user data (encrypted or otherwise) to a remote server.

All the information you share with any SaaS websites is stored on their servers, accessible to you behind a username and password. That means all the thoughts and updates you post, all the messages you send, all the personal details you add to your profile, all your purchases and transactions, all your payees and accounts, are stored on servers controlled and managed by the SaaS.

No matter how secure you make a website, there are quite a few weaknesses of users [1] (such as gullibility, oversight, and many more) that can still be exploited. Therefore, it is extremely important that users are made aware of good security practices so that these attacks are mitigated.

In the sections that follow, I will try and outline as many of these SaaS-related privacy concerns as possible.

ToS and privacy policy

When you sign up for an account for a particular SaaS, one of the things it requires you to do is agree to the Terms & Conditions and accept the Privacy Policy. Almost all of us click the checkbox without bothering to read anything. Due to legal ramifications, companies will always specify their data-sharing policies in their Terms of Service (ToS) and Privacy Policy documents.

In some cases, some companies might even willingly compromise a user's privacy through data-sharing policies that are harmful to the user's privacy. However, since most users don't bother to educate themselves, these companies often manage to get away with it.

Example

A recent example would be the furore caused by a popular photo-manipulation app known as FaceApp. Users who downloaded the app and signed up were shocked when they realized that, according to the Privacy Policy, they had consented to share their data and giving the company all the rights over any images created by using the app! In other words, all images created using a photo app were automatically licensed by FaceApp for free and in perpetuity!

Sadly, due to the one-way nature of the transaction, there is no way to review and revise the ToS or the privacy policies presented by companies – it is a binary exchange in which you can either agree to the terms presented or refuse to use the service in its entirety.

Some courts have ruled that the ToS is not strictly enforceable if they happen to violate the fundamental rights of users. However, in most cases, the terms of service are usually accepted as a binding agreement between the user and the service provider.

Read the Terms of Service; most companies offer a simple language version of their terms of service, where they outline and explain in simple words the terms on which they provide the service to you. These are usually made available at the bottom of the website, or can be found by using the search function on the SaaS website.

Alternatively, you can use the excellent service named Terms of Service; Didn't Read, (abbreviated to ToS;DR) which classifies the terms of service of several commonly used SaaS on a decreasing scale from class A to class E. The service is available as a website and as a browser extension and can be accessed by scanning the QR code displayed on the rightside of this paragraph.

[QR Code: https://tosdr.org/]

Service reliability

For a SaaS to be considered reliable, the two most important things to consider are the security and stability of the software. Software that can be easily breached by external adversaries will not survive in the market. Software that is frequently unavailable will also not survive in the market. However, a SaaS-based application that achieves a significant level of popularity (and thus, reliability) will also suffer from adversarial attacks from actors looking to breach into its data.

Maintaining reliability is, thus, a constant endeavor for any SaaS-based application looking to establish itself in the market. Conversely, a SaaS that cannot ensure reliability will be forced to stop operations and cease service.

What happens to your data if a particular SaaS that you rely on decides to stop operating? Can you port your data to another similar provider? Will either SaaS (the one that is shutting down vs the SaaS that you are looking to move to) provide mechanisms to move the data from one to the other? Or is it simply enough to provide a way to download all your data?

Example

Recently, Google Plus announced that they would be shutting operations and users were provided instructions to download their personal data using Google's Takeout service. While this was a great option for ardent users of Google Plus, it was mostly an empty solution because the downloaded data could not be re-uploaded to any of the other SaaS available in the market.

Another similar example was when the popular Google Reader decided to cease operations. In that case, however, other similar SaaS applications such as Feedly, and more, stepped up to provide an easy way to import people's existing Google Reader subscription lists to their accounts.

Security and transparency

Imagine being told that a particular lock is the best and the strongest until it hits the market and someone managed to break it on the first day using just a simple, cheap screwdriver! How embarrassing, isn't it?

In this scenario, the lock manufacturer relied on the most common principle of security, which is security-through-obscurity. By not revealing the kind of security implemented, the manufacturer hoped to dissuade adversaries from breaking into the lock. However, all applications of security-through-obscurity are almost always subjected to brute-force attacks -- in this case, the screwdriver.

A better approach to security, rather surprisingly, would have been the security-through-transparency approach.

Think about it: if the lock had been subjected to rigorous tests and audits by a competent external third-party, there is a good chance that someone would have found that the lock was vulnerable to brute-force screwdriver attacks much earlier!

Similarly, a competent SaaS-based application or website will ensure maximum security of any and all user data by allowing it to be thoroughly tested and audited by both internal stakeholders as well as external experts. Examples of this behavior can be seen with a lot of popular social networking websites and applications such as Facebook, Instagram, WhatsApp, GitHub, and many more. All of them offer bug-bounty and responsible disclosure programs for external security researchers, a.k.a. ethical hackers.

Getting these ethical hackers to communicate such exploits to the developers and maintainers of the software first allows the developers of the software to fix it before malicious actors are able to take advantage of it.

As I have said constantly, security is not an end goal to be achieved; it is a state of awareness that needs to be constantly reinforced. True security is when you can successfully adapt to any threatening circumstances that may develop with the passage of time.

Security breaches and response

Regardless of whether your SaaS chooses security-through-obscurity or security-through-transparency, your SaaS must have a standardized protocol to respond to security breaches.

Thankfully, more and more regulators across the world are stepping up and making it mandatory to inform users within a reasonable timeframe as a matter of legal compliance.

For instance, the RBI fined Yes Bank to the tune of USD 1 million for failing to notify its users of a 2016 breach that put 32 lakh debit cards at risk. Europe's GDPR (General Data Protection Regulation) laws that went into effect on May 2018 requires companies to notify regulators of breaches within 72 hours, under threat of a maximum fine of 2% of worldwide revenue.

No SaaS is so perfect as to stay successfully unbreached forever. However, a good, competent SaaS will have a properly documented response plan in place with instructions on how to triage and contain the situation, assess the severity and damage, notify the affected users, and educate them on how to prevent this from happening in the future.

Example

Recently, in March 2018, a bug was found in Google Plus by the developers of the SaaS and (according to them) was immediately patched. The discovery and patch were both left undisclosed by the developers who claimed that no data was leaked according to their investigation.

The incident would have gone completely unnoticed were it not for the Wall Street Journal who revealed it in October 2018 -- a full seven months after the incident.

Security updates

There have been occasions where vulnerabilities were found at system-level or hardware-level that affected a wide variety of devices and services and not just a specific SaaS. In situations such as these, it is extremely important to ensure that the SaaS provider updates to the latest patch in a quick and timely fashion.

For instance, the vulnerability nick-named Heartbleed was a serious vulnerability in the OpenSSL cryptography library that could compromise secret keys generated by this library and allow attackers to eavesdrop on encrypted communications. It was introduced into the software on 14th March 2012, but it was only made public on 7th April 2014, with the patch being released on the same day.

Note

The OpenSSL library is used by webservers such as Apache and nginx, which constitute about 66% of all active sites on the internet, that is, 66% of all active sites on the internet were immediately vulnerable to this bug.

Furthermore, email, servers, VPNs, and a wide variety of desktop software that used the vulnerable version of OpenSSL was also affected.

In the aftermath of the revelation of this vulnerability, it was urgent that all applications (SaaS-based and otherwise) were patched with the update to prevent further damage. Companies and individuals across the world scrambled to patch their systems. However, there is a fair chance that some systems may have been left unpatched due to ignorance, inertia, or (worse) plain incompetence.

If your SaaS provider falls into the category of people who did not patch their systems, where does that leave you and your data? It also raises the question: should you continue to have an account with said SaaS provider?

Data access

Typically, users of a SaaS-based application or website may choose to access their data in one of two ways: online or offline.

Allowing a SaaS to be accessed online is definitely a huge convenience -- since it can be accessed from virtually anywhere on the planet. However, that is also what makes it significantly more insecure. For instance, what happens if you log into a SaaS account, for example, a shopping site like Amazon, on a browser in a library or a cyber-café and forget to logout?

Offline SaaS access can be considered to be marginally more secure. However, since it stores your SaaS data on your local machine, the data is only as secure as you can make it.

In either case, the SaaS needs to ensure that the data being displayed to the user is:

Securely stored

Securely transported

Within all applicable legal framework

The last point is particularly important because of the complications that arise when data crosses borders - which it inevitably does when it travels over the internet. For example, Switzerland, a country that guarantees the right to privacy in its constitution, has made it mandatory by law for SaaS providers to store all of their data within the borders of Switzerland.

A SaaS that does not ensure secure storage and transport of data and does not respect the legal framework will end up losing the trust of one or more of its three stakeholders -- the consumer, the investors, or the government.

Example

An example of this is watching movies on Netflix.

The movies are intellectual property that Netflix temporarily licenses, and it needs to (reasonably) ensure that the movies cannot be copied without permission -- either from their servers or while being streamed to the user. Moreover, since the licenses acquired by Netflix are geographically-specific, Netflix needs to ensure that content licensed for India does not get streamed to subscribers who do not have a Netflix India subscription.

RohitRecommends

In recent times, several regulatory bodies have developed frameworks to streng then the privacy rights of internet users, especially users who sign up with various SaaS providers. These frameworks serve as an excellent guideline for checking and tuning privacy settings as well.

Therefore, keeping in mind the privacy concerns I noted above, there are a bunch of actions that I would strongly recommend for SaaS users. Each of these actions requires you to sign into a specific SaaS provider and locate the corresponding setting to execute the recommended action.

In other words, we'll be using generic terms (such as My Profile) to describe the setting, but each SaaS provider may use slightly different terminology (such as Account Details or Profile Details) for the same. I advise you to spend some time carefully working through this checklist to ensure optimum privacy (or maximum privacy) for your profile data stored with the SaaS provider.

As you read through the following sections, you will also note that I am not providing specific actions to take for mitigating privacy threats on these SaaS websites. This is primarily because the actions will differ from person-to-person and also because it will also differ depending on individual circumstances.

For instance, a person looking to be forgotten by the internet might want to either delete or randomize/anonymize their information. However, for most people, it probably makes sense to keep these personal details filled in -- especially on shopping and financial SaaS websites -- to save themselves a bit of time and typing during future logins.

Types of SaaS

Ideally, in this section, I should be providing you with specific steps, techniques, and/or tools to tweak the various privacy settings with all the SaaS websites that you might have signed upon. However, there are so many of them that it obviously makes no sense for me to go into explicit detail for each SaaS website specifically.

Thankfully, most SaaS websites follow a similar pattern for designing their account settings, that is, the section of the website that allows the end-user to make the changes that impact the privacy of their data and security of their account.

Therefore, my recommendations will be designed to give you a broad idea of where to look and what to look for, so that you can conduct your own investigations, draw your own conclusions, and execute them in a way that ensures optimum privacy of your personal data.

The best way to get maximum utility for this chapter would be to follow all the recommendations given in this chapter for each one of your SaaS accounts.

IMPORTANT: Scoring Instructions for this section…

In the section above, where I detailed the different types of SaaS, I have provided common examples of various SaaS websites which fall in that list. Read through the common examples in each category and make a detailed list of all the SaaS that you may have signed up for.

Alternatively, search your email inbox for words such as registration, account details, or similar and then make a list of all the websites that have sent you registration emails. Usually, these websites send emails from a no-reply address, so using that as a search term might yield a few results, as well.

Info

Once you have the list, here's what you'll need to do:

Identify and categorize all your SaaS accounts into one of the following four categories: social, shopping, financial, and other.

Go through your list one-by-one and open the Settings and/or Profile page for that specific SaaS account.

Follow the recommendations given below for each one of your SaaS accounts, as per your needs and requirements.

Keep a running tally of the points earned for each of the SaaS websites – you'll need it to calculate your final score for this section.

Regardless of how many sites you have signed up for, award yourself the average of the points tallied (rounded down, not up) for the recommendations followed for all the sites in your list. For example, if you deleted your Facebook account, made your Instagram account private, and anonymized your Twitter, Reddit, and StackOverflow accounts, that earns you 5+2+3+3+3, that is, 16 points.

Averaged over 5 SaaS websites, that's just over 3 points per site, which is how much you should award yourself once you complete this section.

BASIC (1 point)

First, make a list of all the important SaaS providers who are likely to have critical and/or identifiable information about you. I define critical and/or identifiable information is information that can be used to cause you physical, mental, or financial harm either directly or indirectly. For example, a silly nickname or poem on your profile may not seem very dangerous, but, in the wrong hands, it could potentially have multiple misuses.

Scan Your 'Public Profile': When you sign up with a SaaS provider, they usually ask you to enter some personal information -- usually your name, email address, and contact number. These details may then be made available to the general public through a public profile, especially in case of social networks. The information on your public profile is visible to the world and, by extension, to search engines. That means, anyone who happens to search your name on Google could end up seeing those details, should they choose.

Some social networks give you the option of keeping your profile private that is, most of the information you provide the social network is shared only with a chosen group of friends or followers and is not available to the general public.

I say most here because some information is still available under specific conditions. For example, Facebook allows you to hide your profile from external search engines, but some (or all) of it might still be visible to other Facebook users. Or, when you mark your profile as private on Twitter, your display name, ID, and bio are still visible. Same goes for Instagram, as well.

While I do believe that no is careless enough to reveal private information in their public profiles, it is surprising how many times I find a revealing tidbit casually tucked away in people's public profiles.

INTERMEDIATE: (2 points)

Anonymize your 'Public Profile': Make a note of what information is visible in your public profile and ask yourself the question: How comfortable am I with people knowing this about me? If the answer to that question makes you hesitate, it is probably a safe bet that you might want to remove that from your public profile.

In fact, if it is not made mandatory by the SaaS-provider, I recommend NOT providing any personal information to these websites. You could try using a fake name, or share limited personal details only if/when absolutely necessary.

Tweak your Privacy Settings: Most SaaS websites will provide a specific link called Privacy Settings or something similar. Under this section, you will find all the options related to the public visibility of your personal data and activities.

IMPORTANT!!

Be aware that tweaking your privacy settings may have a significant impact on the way you experience the SaaS, especially in case of social SaaS.

If public visibility of your activities on the SaaS is not important to you, then I recommend setting your profile to private if the SaaS allows it. This will ensure that your activities are visible only to a limited set of users that you can control.

Some SaaS websites may also provide additional settings to tweak the visibility of specific behaviors on the website. For example, Facebook and LinkedIn allow you to choose which of your actions gets shared on your public profile.

Security settings: Most SaaS will also provide a specific link called security settings or something similar. Here, you can find options to reset your password and change your security question.

Use your preferred password manager and change your password to a more secure one, ideally with a length of 20 characters or more. Repeat this process every 3-6 months, at a minimum.

If the SaaS allows it, change the answers to your security questions to something non-obvious. For example, if your security question is, What was the name of your first pet? and your security answer is Fifi , change it to something completely random, such as your favorite Marvel character (Thanos) instead [2] .

If the SaaS allows it, enable multi-factor authentication (MFA) on your account. This acts as an additional deterrent for attackers trying to gain access to your account if your password gets leaked. Use one of the authenticator apps I recommended in the chapter on smartphones.

Note

Note that if you enable MFA, some websites/smartphone apps will ask you to provide your mobile number as a fallback alternative in case you don't have access to your authenticator app. I recommend doing this only for the sites you trust absolutely.

Payment information: There is a good chance that you have purchased something over the internet at some point in time. There is also a good chance that you paid for it using an online payment option such as a credit/debit card, netbanking, UPI or a third-party payment app. Almost all SaaS websites will offer you an option allowing you to store your payment information on their websiteas a 'convenience', but I would recommend against it.

Think about it, would you keep your wallet at your local kiraana just to avoid the hassle of carrying it to the shop every time? Then, why would you want to do that with a SaaS provider?

Look for the section that refers to payments, or wallet, or a similar term that might indicate the section where your payment information is stored. Delete any previously stored payment information.

If you have an active subscription with the SaaS website, you may be required to keep at least one payment method on file. In some cases, not having a payment method on file might result in stoppage of service. You need to make sure that the payment method you choose has an upper limit on spending -- whether through the SaaS settings or the settings of the payment method [3] itself.

This way, if a malicious actor manages to access your account somehow, any expense above the upper limit will be denied, and you'll receive a notification before any of your money is spent.

ADVANCED (3 points)

One way to enhance your privacy on a SaaS website to replace your details in the Privacy settings with random/anonymous data [4] . Note that, this does not erase/change anypast interactions logged with the SaaS website. For example, if you change your username on twitter, your previous tweets are still searchable using your old username, but the results will display your new username.

EXPERT (5 points)

If you're looking to become completely anonymous/invisible, then a good way to begin your anonymization journey is to delete any SaaS accounts that you don't use regularly.

Be warned that deleting SaaS accounts is often quite difficult and requires jumping through many hoops. There are a few companies that offer privacy protection services;that is, they track the internet for any presence of your identity and ensure that those mentions are removed. These services may either be do-it-yourself or paid or a combination of both.

A good place to start would be to check out the justdelete.me [5] service created and maintained by a bunch of volunteers, available here:

https://justdeleteme.xyz/

You can scan the QR code given to the right of this paragraph and open it in a browser on your device. This is a DIY service that provides you direct links to the delete account pages (and, in some cases, instructions) for deleting your account from various SaaS websites.

Alternatively, you can check out Abine's DeleteMe service, which provides a similar (but paid) service for deleting your information from various data-brokers. Scan the QR code given to the right of this paragraph and open it in a browser on your device or go to:

https://www.abine.com/deleteme/

The fewer the number of accounts you have on the internet, the lesser are the chances of your personal information getting leaked by maliciousactors.

SaaS privacy concerns

If a SaaS website were to suffer a breach or if your username and password were to leak somehow, all of these details would lie exposed to * anyone * who knows your username and password.

Of course, the onus is primarily on the SaaS provider to ensure that these security concerns are acknowledged and, if possible, addressed. However, you, as a user of the SaaS website, can also take some steps to mitigate the effects of a breach of privacy that might happen due to one of these concerns being realized.

To that end, here are some recommendations on evaluating a SaaS website on the basis of the various security and privacy concerns I outlined earlier in this chapter.

META

IMPORTANT!! Scoring Instructions for this section

You'll notice that the recommendations for each of the privacy concerns outlined in this section is exactly the same -- delete your account on the SaaS website or anonymize any personal details you may have provided them. You'll also notice that the evaluations questions require varying levels of knowledge of the associated subject matter.

That's why each section carries its own point value since the difficulty of the corresponding subject matter outweighs the simplicity of the recommendation.

All associated point values have been clearly stated next to each of the section titles.

ToS and privacy policy (BASIC, 1 point)

Evaluate your SaaS by asking the following questions:

Did you easily understand the ToS and the Privacy Policy put forth by the SaaS?

Does the SaaS have a class A or class B rating on the ToS;DR website?

Can you import this downloaded backup to another, similar SaaS without requiring expert intervention?

If you answered no to one or more questions, then you may need to consider deleting/anonymizing your account on this SaaS website. Use one of the recommended actions mentioned in the previous section to either anonymize your personal details or delete the account associated with this SaaS.

Service reliability (ADVANCED, 3 points)

Evaluate your SaaS by asking the following questions:

Can you backup all of your data on this SaaS website and download it to a local machine?

Can you view the downloaded data without requiring advanced technical knowledge?

Can you import this downloaded backup to another, similar SaaS without requiring expert intervention?

If you answered no to one or more questions, then you may need to consider deleting/anonymizing your account on this SaaS website. Use one of the recommended actions mentioned in the previous section to either anonymize your personal details or delete the account associated with this SaaS.

Security and transparency (EXPERT, 5 points)

Evaluate your SaaS by asking the following questions:

Do the SaaS offer a bug-bounty program for ethical hackers?

Does the SaaS regularly provide security updates and proactively disclose security incidents?

Does the SaaS proactively deploy the latest security practices and phase out older ones regularly?

If you answered no to one or more questions, then you may need to consider deleting/anonymizing your account on this SaaS website. Use one of the recommended actions mentioned in the previous section to either anonymize your personal details or delete the account associated with this SaaS.

Security breaches and response (INTERMEDIATE, 2 points)

Evaluate your SaaS by asking the following questions:

Has the SaaS suffered a data-breach any time during the time it has existed?

Did the hear about it from an official account or from a third-party?

If data was lost or stolen, was the SaaS website able to recover both the data and the trust of its users?

If you answered no to one or more questions, then you may need to consider deleting/anonymizing your account on this SaaS website. Use one of the recommended actions mentioned in the previous section to either anonymize your personal details or delete the account associated with this SaaS

Security updates (EXPERT, 5 points)

Evaluate your SaaS by asking the following questions:

Was the SaaS affected by any of the superbugs that were recently discovered?

Did the SaaS take immediate steps to mitigate the threat resulting from the superbug being available openly in the wild?

Did the SaaS roll out patches and/or switch to more secure alternatives?

If you answered no to one or more questions, then you may need to consider deleting/anonymizing your account on this SaaS website. Use one of the recommended actions mentioned in the previous section to either anonymize your personal details or delete the account associated with this SaaS

Data access (ADVANCED, 3 points)

Evaluate your SaaS by asking the following questions:

Where are the remote servers for the SaaS located?

Have any of the local governments tried to petition the SaaS for user data?

Has the SaaS transparently revealed what user data was turned over to authorities?

If you answered no to one or more questions, then you may need to consider deleting/anonymizing your account on this SaaS website. Use one of the recommended actions mentioned in the previous section to either anonymize your personal details or delete the account associated with this SaaS.

Conclusion

When it comes to creating accounts on SaaS websites, the saying, Less is more is probably the perfect recommendation anybody could give. Whenever a new website or a new service is announced, we often feel the need to rush and reserve a unique identity on that website or service for ourselves, just so that we don't miss out on it.

I'll be the first to admit that the desire to own your own unique piece of the internet real-estate can be overwhelmingly tempting. However, every new identity you create on the internet erodes your chances of staying anonymous and further adds to the risk of leaking your personal information. Every new public profile means an additional tidbit of your data gets added to the internet. It means that the data-brokers on the internet get to add another piece to the jigsaw puzzle that is your identity.

Signing up for a new SaaS website just because all the cool kids are doing it is a bad idea. Unless you can ensure complete anonymity with every

sign up, I'd recommend that you refrain from signing up for accounts that you don't really need.

I mean, is it really important that you get the username cooldude69 before someone else does?

---

[1] For instance, with email, phishing is a kind of an adversarial attack that relies on the weakness of the user rather than a specific vulnerability of the email website portal itself. The login information is (unknowingly but) ‘willingly’ provided by the user to the adversary in the course of the attack.

[2] You can add this information as a note in the password manager itself. That way, you don’t have to remember this information and it is still available whenever you need it.

[3] If your banking app allows it, you can create a separate wallet with limited amounts specifically for the SaaS to ensure a hard upper-limit on spending.

[4] Although, some sites like Facebook insist on a real-name policy and do not take kindly to fake/anonymous/random names, so beware!

[5] The original service is still available at justdelete.me and is still operational, although it seems to be under the control of BackgroundChecks.org

Chapter 12

Networks: Connectivity and Internet

Introduction

While the most common metaphor for the internet is a series of interconnected tubes , a better metaphor would be that of an open bazaar. The websites are stalls, and everyone uses the services of a translator to speak the language of the sellers. All conversations, transactions, and interactions happen through the translator. Since you can't speak the language yourself, you can only hope that your translator is honest with you.

You may have figured out by now that the translator in this analogy is the network over which your devices communicate. The network protocol is analogous to the language used by the translator and the information you provide the translator may or may not always remain private; for all you know, the translator may be wearing a hidden mic!

So, how do networks function?

When it comes to transmitting data over the internet, networks have a pretty simple job -- to carry information from one point of the network to the other. Most descriptions of networks portray the concept as foot-messenger ferrying letters to and from different addresses.

However, the actual execution is a lot more complicated. Since the network has no memory, that is, it has no way to remember what a device looks like. Instead, the network actually relies heavily on the device identifying itself accurately and honestly.

Surprised? Here, look at how the foot-messenger scenario * actually * looks like in terms of information being sent over a network:

You write a letter, put it in an envelope, write the address, and give it to the foot-messenger.

The foot-messenger takes the letter and knocks on every door that they can find, gives them a copy of the letter and asks them if the address refers to their house.

Every house is expected to answer the foot-messenger’s question truthfully. If they are not the rightful recipient, they are expected to trash the letter immediately.

Once the foot-messenger finds the right house, they deliver the letter and wait for a response.

The foot-messenger takes the response letter and knocks on every door that they can find, gives them a copy of the response letter and asks them if the address refers to their house.

Every house is expected to answer the foot-messenger’s question truthfully. If they are not the rightful recipient, they are expected to trash the letter immediately.

Once the foot-messenger finds the right house, they deliver the response letter and wait for the next letter to be delivered.

I hope you can see the inherent privacy issues in this communication design.

A device may choose to misrepresent itself as the rightful recipient of a message.

The foot-messenger (or their evil twin) may themselves read the contents before proceeding to the next step.

These two scenarios are the primary attack vectors to keep in mind when considering the privacy issues within the network. I'll discuss them in further detail in the #RohitRecommends section of this chapter.

Wired networks

Wired Networks connect devices to each other and the internet using physically wired connections.

Typically, wired networks are seen in homes, offices, and cyber cafes and they make use of Ethernet cables, network adapters, and routing devices (such as hubs, switches, or routers) to share a single internet connection with other devices on the same network. Connections to the internet may be made over broadband, ADSL, or fibre-optic network depending on the technology employed by the ISP providing internet access. For instance, local ISPs typically provide internet over LAN or cable broadband, whereas ISPs like JioFiber, Airtel, andmore utilize their own fibre-optic network to deliver internet to your home. Wired networks typically offer superior performance as compared to wireless networks but at the cost of portability.

Wireless networks

Wireless networks connect devices using electromagnetic waves following a specific communication standard such as Wi-Fi 802.11, GSM, Bluetooth, and more. Wireless networks are typically used in homes, offices, and public places and they can be used to provide users with internet connections on their portable/handheld devices.

Wi-Fi/WLANs

Most homes and offices employ the 802.11 Wi-Fi or Wireless LAN (or WLAN, for short) which involves sharing the internet connection acquired over a wired network by using a wireless internet router. However, thanks to recent technological developments, telecom services providers now provide their customers with hi-speed 4G LTE networks, with browsing and downloading speeds comparable to (or better than) most WLAN/Wi-Fi and Broadband speeds.

Wireless networks suffer from the problem of reliability because they are subject to interference from other electromagnetic emitters and also because of theoretical limits on their propagation, strength, and carrier capacity. Wireless networks, especially WLANs, are also less secure as compared to their wired counterparts, as we will see in the next section.

GSM

GSM stands for Global System for Mobile communication, and it is the wireless protocol on which 2G, 3G, 4G LTE, and 5G is delivered to compatible devices. GSM provides end-to-end security and confidentiality of the subscriber by assigning temporary ID numbers and applying advanced techniques such as robust encryption algorithms, and frequency-hopping to maintain the privacy of the communication.

However, its encryption was leaked in 1994, and multiple vulnerabilities have since been discovered that indicate that GSM is as susceptible to intrusion and malicious attacks as any other wireless network.

Bluetooth

Named after a tenth-century Norse king Harald Bluetooth, this technology was primarily conceived as a low-cost, low-power method to develop wireless headsets that could transmit and receive data over short distances, short-wavelength UHF radio waves. The most popular implementation of Bluetooth is the wireless control and communication between mobile devices and receiving units such as headsets, vehicles, and other devices.

Although versions of Bluetooth after version 2.1 have better encryption protocols, several vulnerabilities have been discovered in various implementations, since as early as 2001.

NFC

The Near-Field Communications (NFC) protocol relies on proximity or taps from/to other NFC-enabled devices to conduct a transfer of data. Connections between these devices are established automatically without any password or credential requirements.

Common attack vectors

In the introduction to this section, I compared the network to a bazaar and the network adapters to a translator/guide helping you communicate with a seller in the bazaar. It is easy to see how your privacy can be compromised if the translator were to, somehow, go, rogue.

In this section, we will look at some commonly used attack vectors for network adapters and routing devices that can be used to compromise your privacy over the internet.

Identification

One of the most important aspects of planning an attack on a network device is acquiring information on the target. This involves figuring out the

identity of the target and searching the target for weaknesses and vulnerabilities. The more information you have about a target, the better you can plan your attacks. Not surprisingly, there are a bunch of tools and techniques that can be used in this phase of operations, that is, to identify the target and its vulnerabilities. The most common among them are:

Port scanners: These are specially designed programs to identify open ports on a device. An open port can indicate a specific protocol being employed by the device and any vulnerability applicable to that protocol can then be used to gain entry into the target system. Think of this as an open door (or window) through which customers can enter or communicate in our bazaar analogy.

Packet sniffers: Packet sniffing is an eavesdropping technique where the attacker is able to intercept all your communication without your knowledge or permission. This is actually much easier than it looks because of the way networks are designed. An attacker can intercept all the data being sent to your device by deploying their adapter in promiscuous mode on your network. To use the same bazaar analogy, this would be like someone being able to clearly monitor each and every interaction between the customer and the shop.

Deep Packet Inspection (DPI): This is a highly-intrusive packet-sniffing technique that involves using automated programs to read the contents of the datapackets that are being exchanged between your computer and the remote server. DPI can be used to extract sensitive information about the victim's online activities and browsing habits. This knowledge can then be used to create a firewall that can interfere or interrupt such traffic, as and when necessary.

It is common knowledge that such DPI-assisted firewalls have used by some authoritarian governments to monitor the activities of their citizens and (either proactively or reactively) curb their freedoms. In recent times, a few ISPs have also taken to using DPI to analyze network traffic and snoop on their users without their knowledge or permission.

Spoofing: Spoofing involves impersonating either a device or an authority to con the victim. In a MAC-spoofing attack, a malicious attacker might impersonate your MAC address to gain entry into your local network, or to install software that works only with certain MAC addresses.

In an IP-spoofing [1] attack, a malicious attacker crafts packets with a false source IP address to fool the victim into sending critical data to the attacker's desired destination. In a DNS-spoofing attack, malicious actors may change DNS entries pertaining to a website either on your local machine or on your network's DNS server, in order to redirect you to the attacker's computer and steal your credentials.

War-driving: This term refers to reconnaissance techniques where malicious attackers attempt to surveil a geographical area to identify available access points physically. Malicious attackers physically drive around with a portable/handheld device to scan areas and map out all the available Wi-Fi access points into a database.

Interception

The interception phase is the phase of an attack by a malicious actor that actually threatens your privacy and your personal data. Some malicious actors may choose an interruption phase instead of interceptions , which aims to disrupt a user's online activities completely.

The actual attack perpetrated by a malicious actor takes the form of either an interception or interruption of the flow of data. Both of these techniques have different end-goals; while interceptions are aimed at acquiring critical information, interruptions are mainly intended to be disruptive. To extend our bazaar analogy, an interception would be if someone were recording everything said by your translator/guide and interruption would be a crowd screaming gibberish while your translator was trying to establish a communications channel with the seller in the bazaar.

Let's look at some of the most common interception and interruption attacks:

Man-in-the-Middle: Also known as Monkey-in-the-Middle and usually shortened to MitM, these attacks involve a malicious actor who is in a position to intercept communications between two networked devices, such as your PC and the remote server. Information sent by one device is intercepted by the man in the middle, that is, the attacker (thus the name) before being passed on (usually after changing it in some manner) to the other device. For an MitM attack to be successful, the attacker must be able to impersonate both devices on either side precisely.

Replay attacks: These are a lower-tier of the MitM attack, where the attacker silently intercepts communication between two devices on a network and replays relevant portions at a later time with the intention of impersonating one of the two devices. For example, replay attacks can be used by a silent MitM attacker to re-login to a user's account after they log out. Or, an actual replay of a user's voice could be used to breach a voice-recognition system.

Smurfing/Flooding: This is a form of Denial of Service (DoS) attack employed by malicious actors to overwhelm a device or adapter on a network. It involves sending a large number of IP-spoofed communication packets to multiple devices on a network. When all these devices reply back to the spoofed IP, the victim's machine slows down to an extent where it becomes difficult to work on it. The Ping flood and Ping of Death attacks are essentially variations of the Smurfing attack.

Wireless attack vectors

While the above attack vectors can be (and often are) used for both wired and wireless networks, there are some attack techniques specific to wireless networks that deserve a special mention:

Malicious networks: Malicious networks are usually created by craftingaccess points that are specifically placed by a malicious attacker to lure unsuspecting victims. Theseare typically waterholes , that is, networks placed and presented in such a manner as to lure the user into connecting to them. Typically, such access points are given lucrative names such as Free Airport Wi-Fi or Free Hotel Wi-Fi and are always unsecured and/or unencrypted.

In some cases, the attacker may even smurf, flood, or jam other SSIDs to further influence unsuspecting victims. Once connected, devices are rendered immediately vulnerable since all communication must pass through this malicious network, thus providing the attacker with a clear MitM view of all the unencrypted traffic.

Evil twin attack: An evil twin attack is quite similar to a malicious network except that it is specially crafted to impersonate a previously connected Wi-Fi AP. The evil twin is the Wi-Fi equivalent of the phishing scam. By conducting a war-driving exercise, a malicious attacker identifies unsecured Wi-Fi access points (APs) and then creates an evil twin for one of the chosen APs.

Sometimes, attackers may also reverse engineer evil twin APs by intercepting the Wi-Fi search scans made by the victim's device to see what other APs the user is trying to probe [2] . If any of them are unsecured, the attacker may use those names to create an evil-twin for the victim.

In either case, the original AP is then smurfed, flooded or jammed while keeping the evil twin alive. Since the evil twin has the same SSID, any devices connected to the original AP can be made to switch to the evil twin thus giving the attacker a clear MitM view of the communication between the user and any remote servers they may be connected to.

WEP/WPS brute-forcing: Brute-forcing refers to the practice of trying out every possible combination of alphabets, numbers, and special characters to break the encryption and find the password to a secured wireless network. A variant of the brute-force attack (and one that is increasingly more commonly used) is the dictionary attack in which the most commonly used passwords are tested first before attempting a pure brute-force attack. WEP is an older form of encryption used by Wi-Fi routers and has since been discovered to be extremely vulnerable to the simplest brute-force attacks. In some cases, WEP-encrypted passwords have been cracked in as little as 5 minutes.

WPS or Wi-Fi protected setup relies on pairing devices by simply pressing a button on two Wi-Fi devices. The encryption, in this case, uses an 8-digit PIN to encrypt the information exchanged between the devices and set up a WPA link. However, a tool called Reaver can brute-force the WPA-encryption without the physical WPS button being pressed. While WPA by itself remains a somewhat secure encryption method, the WPS encryption key has been proven quite susceptible to brute-force attacks by the Reaver tool.

Note that, given a bit of time, money, and patience, brute-force attacks can also be used to recover passwords encrypted using strong(er) encryption such as WPA and WPA2. Open-source tools such as aircrack-ng have made the entire process as simple as downloading a file, extracting it, and running it on your system!

Jamming: Jamming is a more aggressive DoS attack in which the RF frequencies (on which the wireless signal operates) are jammed using external interfering signals. A simple example of inadvertent jamming is the sudden loss of Wi-Fi when the microwave is switched on. Malicious attackers may use this technique to induce artificial jamming and then lure unsuspecting victims with a rogue AP or an evil twin attack.

Note

All of these wireless attack vectors are applicable for the other types of wireless protocols as well, that is, GSM, CDMA, Bluetooth, and NFC. Ever since the design for GSM encryption was leaked in 1994, various security researchers have been able to employ most or all of the aforementioned common attack techniques such as packet sniffing, jamming, smurfing, and different kinds of MitM attacks.

Bluetooth

There exist several different attack vectors for the Bluetooth protocol, not all of which bear resemblance with the more generic wireless attack vectors described in the section above.

Here are a few popular Bluetooth attack techniques commonly employed by malicious attackers:

Bluejacking: Bluejacking, by itself, is a relatively benign Bluetooth attack that involves sending unsolicited messages to nearby Bluetooth devices. The malicious variant of a bluejacking attack involves sending the contact file (usually a VCF file) to an unsuspecting victim. If this contact file is added to the phonebook, any files sent by the contact may be automatically opened by the device, thus elevating a simple bluejacking attack into a backdoor attack.

Bluesnarfing: Bluesnarfing involves unauthorized exploitation and theft of information from a wireless device through its Bluetooth connection. Attackers may download your contact list, your calendar, and other sensitive data using your device's Bluetooth connection.

Bluebugging: Bluebugging involves completely taking over a victim's mobile phone by acquiring unauthorized access via its Bluetooth connection. Attackers will often pose as a known Bluetooth device (for example, your headphones) and attempt to pair with your Bluetooth device. Once connected, the attacker acquires full control over your phone and can use your phone to place calls, listen to calls, read messages, read emails, use your phone as a modem, and even track your location!

Blueborne: Possibly the most dangerous attack vector, Blueborne was a comprehensive security threat that exploited multiple vulnerabilities in the Bluetooth protocol. A phone targeted using Blueborne could be completely hijacked with no user interaction, […] and does not require any preconditions or configurations aside fromthe Bluetooth being active.

Blueborne affected almost all devices, from phones to audio systems to desktop PCs across multiple vendors, including Google, Microsoft, Apple, Amazon, LG, and Samsung -- just to name a few. All of the vendors involved immediately patched the vulnerabilities that were revealed, but unpatched devices could still be vulnerable to Blueborne attacks.

Note

Technically, even though Bluetooth can be considered a wireless network, it is treated differently (by developers and attackers both) due to the way its protocol is designed.

NFC

Drive-by: You may have seen the video of the man in a convenience store making a payment by tapping the payment device to an unsuspecting user's back pocket, where the victim's contactless card was probably kept in a wallet. If you haven't, you can check it out here:

[QR Code: https://www.youtube.com/watch?v=DocbhfRMrLo]

These contactless cards issued by banks are based on the NFC protocol, which is how the man in the video is able to charge someone else's card by simply tapping it against their pocket. For a drive-by to be successful, the distance between the two NFC devices needs to be as small as 4-6 cm, which is difficult but certainly not impossible to achieve.

RohitRecommends

Ordinarily, I would outline each one of the different types of networks and specifically describe mitigation and prevent techniques to ensure that your networks were protected from the various attacks described in the chapter so far.

However, a large part of staying safe on networks involves following some basic hygiene, which I have discussed in this section. There are very few specific recommendations I can give to secure each of the network devices and protocols separately. I'll try and enumerate them separately in this section, wherever possible.

The recommendations in this section have been designed to take into account all possible issues, vulnerabilities largely, and attack vectors discussed in this chapter. While some issues discussed in the chapter require specific intervention, most of the issues can be resolved by following the instructions given under various recommendation levels below.

BASIC: (1 point)

Staying safe on the internet is mostly based on common sense. Think of it as visiting a large city in an unknown country. As long as you stick to the popular spots and don't venture into shady alleys, you should be safe. All the common sense you would apply in such a situation is exactly the kind of common sense you need to apply on your networks as well:

Safe browsing habits: While 'safe browsing habits' is certainly a broad concept, I have discussed a lot of them in the various #RohitRecommends sections sprinkled across the book. These habits won't come naturally to most people -- in fact, you'll need to follow them in the beginning consciously, but once you get used to it, it'll become second nature to you!

Antivirus andfirewalls: Regardless of which device you use, it is advisable to have a decent antivirus and a firewall deployed on your system. Most operating systems these days even provide their own home-baked solutions. The default Windows Defender software that comes pre-installed on all Windows 7, 8.1, and 10 systems is a pretty good antivirus and firewall solution. On Unix-based systems such as macOS and Linux, firewalls are slightly more complicated than just flipping a switch.

Switch off radios and sensors when not in use: When you're not using them, turn off your Wi-Fi, mobile data, Bluetooth, NFC, GPS, and any other wireless network that you might have left switched on. One, it will help you conserve your battery life and keep your phone alive for longer during the day. Two, if a specific radio isn't broadcasting; the chances that someone hijacks your device go down drastically!

Specifically, check your Bluetooth settings and ensure that your phone is not in Discoverable mode by default! Furthermore, if you use NFC-enabled contactless cards, encase them in RFID-safe covers to prevent your card from being used in drive-by attacks like the one mentioned above.

Do NOT connect to ANY unsecured networks or devices: It is tempting to connect to something that has the word free in its name - hey, who doesn't want to save a few bucks, right? But, the free Wi-Fi may be a rogue AP waiting to MitM your browsing and steal your credentials.

Even if the free Wi-Fi is offered by a person you trust, do not succumb to the temptation. Instead, help them enhance their security by teaching them how to secure their Wi-Fi by setting up WPA2 authentication with PSK (Pre-Shared Key) on their wireless router.

Essentially, it is better to use your own mobile data rather than connecting to an unknown, unsecured network.

Do not accept, download, or open any files from any unknown devices or persons: Often, all it takes to install a backdoor on your system is opening a random file with unknown origins. We saw earlier, in the Android chapter, that malware can be installed on your phone by simply opening a PNG file! Similarly, there exists software that can hijack your device by sending seemingly innocuous files through your Bluetooth connection. Until recently, there existed vulnerability in Airdrop (on iOS and macOS) that allowed an attacker to silently install a malicious app by simply sending a file to an unsuspecting victim.

INTERMEDIATE: (2 points.)

At this level, I'd ask you to follow all the instructions given under the BASIC recommendation level and also implement the following additional recommendations:

Update the firmware on all devices on a regular basis: A firmware is simply an operating system specific to a device that allows the device to perform specific functions. In that sense, Windows is a firmware for your desktop or laptop; Android OS is a firmware for your Android device; iOS/macOS is the firmware for your Apple device, and so on. Every manufacturer releases updates to firmware whenever serious vulnerabilities are found. Always ensure that you check for firmware updates for all your devices regularly and install any security updates immediately.

Invest in a good antivirus and firewall: There are good antivirus options available that are both free and paid. If you are willing to invest some money, consider purchasing a license for a good antivirus and firewall. A lot of internet security software development companies will offer a bundled product at reduced prices. You might even get a good deal if you purchase them during the Cyber Monday sale or similar.

Some popular options for antivirus and firewalls are mentioned below

Antivirus: BitDefender and Trend Micro

Firewalls : ZoneAlarm and Comodo

Please note that these are not the only recommended options; these are merely the most popular ones. You may choose to opt for a different antivirus and firewall if you so choose.

Monitor your network: To understand what is wrong with your network, you need to have a good idea of how it behaves when it is right. Monitoring your network on a regular basis will give you a baseline definition of what normal and regular look like, on your network. Any deviation from these baseline values should be investigated and acted upon quickly. For example, if your Netflix appears grainy too often, it could mean some application is hogging a majority of your network bandwidth. Or, if your antivirus suddenly refuses to update to the latest virus definitions, no matter how much you try, it could mean that your system has been infected by malware.

Switch to a secure DNS: In recent years, multiple cloud DNS services operated by major players such as Google, IBM, OpenDNS, Cloudflare, and many more, have become available promising greater security, faster resolution, and increased privacy. Some of these services also provide additional features, such as secure communication, ad-blocking, and parental control.

The catch is that your DNS queries are sent to these servers, who can then utilize this data in whatever way they choose. Although most of them claim that they do not store any logs of the DNS queries, there is usually a 24-hour wait time before the logs are deleted. Regardless, I'd still strongly recommend switching to one of these DNS servers.

Among the many options available today, Cloud flare's 1.1.1.1, Quad9 (9.9.9.9) by IBM, and Google's 8.8.8.8 are options you might want to consider seriously. Those looking for ad-blocking might want to look at the Blokade or AdGuard apps, while Comodo SecureDNS (8.26.56.26), and OpenDNS Home (208.67.222.123) both offer parental control options as a (usually free) service for registered users.

ADVANCED: (3 points.)

The following recommendations require you to invest both time AND money into securing their networks, that is, more for organizations than individuals. However, if your home contains a lot of IoT devices, you might want to follow them too:

Intrusion Detection and Prevention Systems (IDPS): There exist options for detecting and preventing all kinds of vulnerability exploits and unauthorized access on your network. These tools are commonly referred to as IDSs (Intrusion Detection Systems) and IPS (Intrusion Prevention System) - depending on the extent of threat-mitigation they provide. These systems monitor the network for any malicious traffic, log relevant traffic information, and (may also) take necessary steps to stop them.

IDPS are available in both hardware and software variants, with both open-source and proprietary options available in the software variant. The hardware variants usually market themselves as Next-Generation Firewall, or Smart Internet Security devices or Hardware Firewalls and are usually designed to be plug and play. The modern versions of these intrusion detection and prevention systems are relatively easy to set up and get running.

Some of the popular intrusion detection softwareare:

Snort (Free and open-source, for Windows and Linux)

OSSEC (Free and open-source, for Windows, macOS, and Linux)

Suricata (Free and open-source, for Windows, macOS, and Linux)

As for hardware firewalls/smart internet security devices, you might want to consider:

Trend Micro Home Network Security

Bitdefender BOX

BullGuard Dojo Smart Internet Security and Privacy Solution

Bear in mind though, these devices are somewhat expensive and are recommended only if you absolutely need to secure your internet browsing. For most home-use cases, using these may be unnecessary and rather extravagant.

Virtual Private Networks (VPN): I've mentioned VPNs in quite a few places throughout this book. A VPN is essentially your network connecting to another network, which then connects to the internet on your behalf. This secondary network, which provides a promise of privacy and anonymity, is called a VPN . VPNs are extremely useful in situations where you suspect (or know) that your network traffic is being monitored by an external agency and you want to bypass their spying eyes.

Note

VPNs differ from proxies because they do much more than hiding/spoofing your IP address. A determined attacker will still be able to snoop on your internet traffic (even if it is proxied) and infer the destination website using a variety of sophisticated techniques.

There are both free and paid VPNs that you can use to connect to the internet, although most free VPNs offer severely limited value by either throttling speeds, or restricting data usage. In some cases, using a free VPN may even cause a privacy nightmare for your due to their policy of sharing your browsing data with third-parties.

While there are several free VPN services that offer good-to-decent value, opting for a paid VPN service will most likely result in a better quality of service. Some important aspects to consider while evaluating a VPN service are:

Privacy and logging policy: Look for VPNs who can offer complete virtual privacy to their customers, that is, they do not store any logs or snoop on any of the data being transmitted through their servers, and ensure complete anonymity for its customers.

Security features: Some important security features to look out for, in a VPN, are kill-switches, encryption of all traffic, and the VPN's track-record on security.

Server locations: A VPN that has its servers in privacy-aware locations such as the EU definitely rates higher than a VPN with servers in places with a poor track-record of user privacy, such as the US, UK, and Australia. The geography of the servers also matters in terms of legal jurisdiction, censorship, and surveillance. Plus, having access to servers in multiple countries allows you to access geo-restricted content, too.

Bandwidth, speed, and throttling: Most paid VPNs offer unlimited speeds with a decently-sized data cap. Most free VPNs will throttle either the data or the speeds or both after a predefined limit. In some cases, VPNs may choose to show ads in exchange for offering you free VPN services.

Device compatibility: You can always set up a VPN directly on your device, but most VPN providers provide a separate app for your device. Ensure

that the VPN provides an application compatible with all your devices and that ititself is secure and not privacy-averse.

Cost vs value: This is arguably the most important aspect to consider while choosing a VPN. While the basic-tier of most VPNs are priced more or less similarly, the differences in the features offered may result in price variations in premium-tiers that may put a certain service(s) beyond your budget.

Keeping all of these aspects in mind, I would recommend the following VPN services as worthy of consideration for a paid subscription:

ProtonVPN

ExpressVPN

NordVPN

Mullvad

The Tor browser: Another layer of privacy can be added to your internet browsingby using the Tor network instead of (or alongside) your VPN provider. Similar to layers of an onion, Tor adds a strong layer of privacy to your browsing by bouncing your communications around a distributed network of relays run by volunteers all around the world.

Here's what Wikipedia has to say about the Tor project:

"Tor is free and open-source software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router". Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays."

Scan the QR code given alongside the above paragraph to open the Wikipedia entry for Tor in a browser tab on your device.

[QR Code: https://en.wikipedia.org/wiki/Tor*(anonymity*network)]

To extend an analogy I've previously used in this chapter, using Tor is similar to playing Chinese Whispers with the seller in a bazaar BUT without any loss of information.

Using the Tor browser is quite easy. Download the file from the official website (i.e. torproject.org) and run the executable file. Follow the instructions shown during the install process. When the installation completes, simply launch the Tor browser by double-clicking the shortcut named Start Tor Browser in the folder where it was installed.

EXPERT: (5 points)

As always, the recommendations under this section must be made under thesupervision of someone who knows these concepts thoroughly. Ensure that you have ample backups before you begin and have a sure-fire way of rolling back any changes that you make from this point onwards.

I take no responsibility if anything goes wrong in your attempt to execute the following recommendations:

DNS over HTTPS/TLS: The DNS over HTTPS (DoH) standard was proposed in October 2018, and it involves querying DNS servers over secure, encrypted channels to ensure maximum privacy by preventing eavesdropping and manipulation of DNS data. The DNS over TLS security protocol is already available and implemented by multiple DNS providers (such as Cloudflare, Google, and Quad9) to ensure user privacy and security.

If you are using Firefox version 62.0 or greater, you can enable DNS over HTTPS as follows:

Type about:config in the URL bar and press Enter.

You'll see a warning. Read it carefully, uncheck the box, and press the button that says, I Accept!

In the input field at the top, type network.try and wait for the rows to get filtered. Look for the row titled network.trr.mode and double-click it.

In the dialog box that pops up, change the value from 0 to 2 , and click OK .

Next, look for the row titled, network.trr.uri, double-click on it, and change it to one of the following DNS over HTTPS providers, listed at this URL: https://github.com/curl/curl/wiki/DNS-over-HTTPS

Finally, search for network.trr.bootstrapAddress , double-click on it, and change it to the IP address of the DNS query server, for example, 1.1.1.1 , if you chose Cloudflare in the previous step.

Scan the QR code given alongside this paragraph to open a blog-post titled Configure DNS Over HTTPS in Firefox on ghacks.net, where steps

described above have been documented with additional details and screenshots

[QR Code: https://www.ghacks.net/2018/04/02/configure-dns-over-https-in-firefox/]

Bespoke NIDS with Raspberry Pi: You can set up a bespoke Network Intrusion Detection System and Firewall using a Raspberry Pi, which will perform the following functions on your network:

Enforce network traffic policies.

Ensure that abnormal packets do not get out or in our network.

DHCP server to distribute network parameters to your LAN.

DNS cache/server to speed up DNS requests and filter out bad DNS queries.

NIDS to detect malicious traffic, such as malware or vulnerability exploits.

Act as a central network monitoring node to watch and debug network traffic.

This method is highly technical and requires significant expertise inthe subject matter, and I would not recommend doing it without expert supervision. If you'd still like to give it a try all by yourself, please look up relevant articles on pfsense, Pi-Wall, and pi-hole to understand the intricacies of setting up a bespoke NIDS and firewall using Raspberry Pi. The QR code given alongside this paragraph points to an article on the Instructables website, which will help you get started with this process.

[QR Code: https://www.instructables.com/id/Raspberry-Pi-Firewall-and-Intrusion-Detection-Syst/]

Conclusion

We've looked at privacy concerns with devices, and we've looked at privacy concerns with services on the internet. However, the most important aspect that goes ignored while considering connections between devices and services is the layer that makes it possible, viz. the network. We often don't give much thought to * how * a device connects to the internet, only that it is able to.

Networks are simultaneously the weakest and the strongest aspects of communicating over the internet. We use different kinds of networks on a daily basis, often without properly considering how secure these networks truly are. We assume that our communication over these networks is non-leaky and that our messages reach the desired destination without any interference.

I hope this chapter has opened your eyes to the possibility that these assumptions may not always hold true, especially in the case of unknown networks.

Just like you shouldn't trust an unknown computer, you shouldn't trust an unknown network either. I get it - free Wi-Fi is tempting. Random files sent by anonymous people over Bluetooth are tempting, but you need to overcome that temptation to prevent the possibility of your device getting infected, or worse, breached.

And, if you absolutely must connect to an unknown network, ensure that you have the right security software set up and properly configured on your device. If you can't avoid it, you need to make sure that you are adequately equipped to prevent it from damaging you and your data.

In simple words, prevention is better than cure, and it pays to be always prepared.

---

[1] MAC-spoofing and IP-spoofing both have legitimate uses in software testing, identity masking, and anonymization.

[2] A popular wireless attack tool called ‘Café Latte’ used this technique to recover cached 128-bit WEP keys, and demonstrated the same at ToorCon 9 in 2007

Chapter 13

Operational Security (OPSEC)

Introduction

OPSEC (short for OPerational SECurity) is a military term to describe the process of ensuring that casual exchange of information between two friendly members of a unit does not accidentally yield critical information to a non-friendly actor.

As we’ve seen in the chapters so far, tiny bits of data can be put together to form a larger picture. We have seen how the entire targeted advertising industry relies on this methodology to automagically create profiles for users browsing the internet. Each website visited, each bit of content posted, each video viewed, each product bought -- everything you do on the internet is used to assign a data-point to your profile. A collection of data points big enough can then be used to make a deterministic evaluation about you.

This is where OPSEC comes in handy.

Broadly speaking, OPSEC is a set of processes and behaviors aimed at ensuring that mission-critical information does not get accidentally shared with an adversary. Wikipedia defines OPSEC as follows:

Operations security (OPSEC) is a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.

[QR Code: https://en.wikipedia.org/wiki/Operations_security]

As a matter of fact, that is also exactly what I have tried to teach you throughout this book. Actions that you don’t particularly think twice about can be used by various adversaries against you. Therefore, in the #RohitRecommends sections at the end of each chapter, I’ve attempted to change either the settings of the system or change your habits. If you followed my recommendations, there is a good chance that you were able to restrict the different kinds of information that your devicesmight have shared with the internet otherwise.

In this chapter specifically, I’ll enumerate and explain some of more rigorous processes and behaviors and help you devise a sufficiently secure OPSEC strategy to ensure maximum privacy of your personal data.

An adversarial approach

In terms of OPSEC, it is safe to assume that any person who receives your data or is in a position to receive it may be an adversary. This adversary may be known, hidden, or unknown . For instance, in terms of browsing the internet, you can define known, hidden, and unknown adversaries as follows:

Known: For example, the remote server that hosts the website you are browsing.

Hidden: For example, the cookie placed by an advertiser that collects information about your browsing.

Unknown: For example, an eavesdropper on your network sniffing all your interactions with the website.

Under OPSEC conditions, you always assume that all three kinds of adversaries can track every action you perform. You must also assume that adversaries will collect several actions and piece together a larger picture by analyzing these actions within the appropriate context.

For example, imagine you work with the military, and you urgently need to call someone, but your phone has just died. You could wait, or look for a phone charger, or search for a public phone, or request a stranger to lend you their phone. One of these actions is highly recommended, and one of them is absolutely not recommended. Can you guess which is which?

I’ll save you the suspense. Waiting is the highly recommended action and requesting a stranger for their phone is absolutely not recommended.

Remember what I said about adversaries? Well, the stranger is an adversary in this scenario. The simple action of using a stranger’s phone revealsat least two pieces of information to the stranger – the number you call, and your physical location to the adversary. A determined

adversary could even read between the lines and extract other useful meta-information from the scenario.

The OPSEC process

It is believed that the US military developed OPSEC during the Vietnam War. They developeda protocol to institute processes to prevent mission-critical information from being accidentally inferred by the adversary by piecing together unrelated bits of information.

The project was initially named Purple Dragon but was eventually replaced by the term operations security that was coined to describe these processes during the Vietnam War.

Scan the QR code given alongside this paragraph to download a PDF of the de-classified issue of Cryptologic Quarterly , and check the section titled, Observations on the Evolution of OPSEC (Operations Security) on page 8.

Also, here's another, telling excerpt from the same report:

The Vietnam War was the catalyst for the development of OPSEC. This war dramatically illustrated the need for OPSEC because the enemy had so much foreknowledge of American activities.

[QR Code: https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-quarterly/remembering*the*lessons.pdf]

The OPSEC process is iterative (that is, to be repeated until all mission-critical information is secured) consists of 5 important steps, as described below:

Identify critical information: You must first establish the information that needs to be protected and understand the reasons why it needs to be protected.

Analyze threats: Next, you must identify potential adversaries, their motivations, and any harmful actions they may execute.

Analyze vulnerabilities: Next, you must analyze your own setup and identify if any potential weaknesses exist that the adversary can exploit.

Assess risks: This step involves exploring the possibility that the adversary manages to exploit the weakness and the fallout of the action.

Apply countermeasures: Now that you have all the necessary information, what can you do to protect your critical information?

While OPSEC's origins may be rooted in the military, this doesn't mean that OPSEC is meant only for military personnel. OPSEC is a behavioral protocol that can be practiced by anyone and everyone. In fact, OPSEC practices come in very handy even in the context of something as banal and mundane as posting a photo taken in your bedroom to social media.

Let's break down this example and evaluate it in OPSEC terms.

Every photo contains embedded EXIF data, which contains highly sensitive information such as the make and model of the device, location coordinates of the place where the photo was taken, and more. To protect this critical information, we need first toanalyze the threats that may affect this critical information.

There are several threats that might arise from this action, but the most immediately identifiable threat is someone (a home invader, a jilted lover, and more) who might be trying to find out where you live. Uploading the photo also renders you vulnerable, since the adversary can use the EXIF data to identify the precise location of your home, thanks to the embedded GPS coordinates. A simple solution to protect your sensitive data would be to use a tool to strip off all the EXIF data from the photo before uploading it to social media!

By answering five simple questions, we were able to identify a useful OPSEC process for action as banal and mundane as uploading a photo to social media. Using these techniques, I have devised a set of instructions in the form of Dos and Don'ts for certain crucial aspects of data privacy in daily life.

In the sections that follow, I'm going to outline these Dos and Don'ts to ensure that your data remains private and secure.

Dos and Dont's

You know by now that OPSEC is a rather detailed investigative process, which involves identifying critical information, vulnerabilities, threat actors,

and implementing countermeasures.

That said, there are a few DOs and DON'Ts that I can definitely recommend. I can state with one hundred percent certainty that these will inevitably form a part of the recommendations generated by any (and every) OPSEC evaluation.

You'll recognize some of the DOs and DON'Ts as instructions that you may already be following from earlier in the book. You can still use this section as a reminder to ensure that the settings haven't changed and everything is as it should be.

Mobile phone subscription

Not all banking apps provide the ability to use an authenticator app to generate the OTP for conducting transactions. In most cases, banks prefer to verify transactions by sending OTPs through text messages or verification calls to the customer. On a smartphone, this means that the OTP can be read by a third-party app that has access to your messages -- clearly, a security risk that cannot be ignored.

With that in mind, the following recommendations could help ensure better security for your financial transactions:

Buy a separate phone connection [1] for different usage purposes. For example, use a non-smart phone for all your banking needs and conduct all transactions using the SMS-based or phone call-based OTP, wherever possible.

Use a basic phone (a.k.a. a dumbphone) for your banking needs. One, no one is likely to suspect the significance of this action. Two, you won't be able to compromise the security if you can't install any apps.

Keep the associated phone number private and exclusive for the corresponding usage needs. Use the banking phone for banking calls, the work phone for work calls, the personal phone for personal calls. Use a dual SIM phone to avoid carrying multiple handsets, if required.

If you decide to use a separate phone for your banking and financial transactions, ensure that the phone number stays as private as possible but also use it regularly to ensure that it doesn't get compromised in a SIM-swap attack.

Device security

Setting up a lock-screen for your device a simple but often-ignored recommendation. The flimsy excuses used by most people for not having a secure lock on the phone, usually range from takes too much time to unlock to forget often the password to what if there is an emergency.

Here's my recommendation: if your device does not have a secure locking mechanism, set it up immediately! Like, stop reading and set it up NOW!

Use the following set of instructions to decide what kind of lock-screen you want on your device:

In terms of security and encryption, a password is more secure than a PIN, and a PIN is more secure than a pattern.

The longer the password, the more difficult it becomes to crack the encryption

Avoid using biometric IDs such as fingerprints, face, and more, to lock, if possible.

If you ever need to decide between using the browser or installing an app to access something, always choose the browser over the app. The browser provides greater control over what personal information is transmitted as compared to an app.

The fewer the apps on your phone, the fewer the vulnerabilities, and the fewer the chances that your phone gets attacked with an exploit.

Ensure that your device has the necessary anti-malware and anti-virus capabilities installed and active on your phone.

In the chapter on smartphones, I have provided a list of recommended apps – ensure that those apps are downloaded and installed on your phone.

To sum it up in simple words: Set up a lock with a difficult-to-guess password on your phone, avoid using biometric IDs, and use good security software.

New signups

The internet sees new services being introduced every day, in the form of websites and apps. Sometimes, these apps are interesting enough to warrant signing up on them. However, every new account you create increases the likelihood that your personal data may get compromised.

One way to combat this is to ensure that you do not share any personal data when you sign up to a new service on the internet. There are several ways to make this happen, and we have discussed quite a few of them in the earlier chapters. Here are a few more recommendations along the same lines:

Use disposable email addresses to sign up for websites you are unlikely to visit again. Mailinator, 10minutemail, and SpamGourmet are my

preferred websites of choice for disposable email addresses.

Ensure that you have complete knowledge of which services automatically shares your information on a public profile.

Use non-identifiable, anonymous usernames and emails like cooldude33 or moonlight44, while signing up.

Avoid giving out your personal email address. Instead, use separate email accounts for each sign up. You could use a mail-forwarding service like boun.cr and 33mail.

Use a strong password, a password manager, and Multi-Factor Authentication (MFA) using a good authenticator app rather than SMS.

Consider using an offline password manager instead of an online password manager. Use separate databases with separate passphrases to store passwords in the contextthat is, Personal passwords in the personal database, Work passwords in the Work database, and more.

It is important not to lose track of the various accounts that get created over time. I would recommend that you execute a clearing-up of inactive accounts at regular intervals of time, say every six months or so. You can even make it coincide with your semi-annual password changing routine, to make it easier to remember.

These are merely a few examples of the various scenarios where you might need to consider adopting OPSEC practices. In truth, there are tons of situations where using OPSEC would be absolutely necessary. There is more than enough content to fill an entire book on the subject, but we'll have to make do with just a small chapter for now.

I'll say just this: OPSEC is a philosophy, not an end goal. Like all philosophies, it requires you to ask a lot of questions and search for answers. Like all philosophies, it teaches you a certain way of life. Like all philosophies, it may give you answers you may not like to hear.

And, like all philosophies, it is entirely up to you how strictly you want to adhere to it.

Conclusion

Throughout this book, in each of the chapters you have read so far, I've given you various recommendations on how to prevent your personal information from being accessed without your consent. I've provided processes and methods of varying levels of difficulty (ranging from BASIC to EXPERT) to combat the unnecessary sharing of data by various devices, services, and the networks that connect them.

Cultivating OPSEC behavior in your day-to-day life essentially involves adopting all of those recommendations and making it into a habit. It involves extensively evaluating the results of each action and finding a suitable option that ensures little to no leakage of critical information.

To put it simply, adopting OPSEC in your life requires extreme awareness of your actions. It requires you to consider each action carefully and evaluate the potential ramifications of the action and then devising counter-measures which will ensure minimal fallout.

Just to give you an example, consider the simple, mundane action of checking your email. Ordinarily, you'd open a browser window, enter the website address, and log in to your account. OPSEC requires that you evaluate each one of these steps, identify threats and vulnerabilities and find counter-measures that protect your personal information. In all likelihood, in this scenario, you'd end up using your TAILS bootable USB or a Whonix gateway to open up Tor browser on a trusted network to log in to your email inbox with a password manager and MFA enabled. It might seem excessive, but that is what OPSEC is all about -- lots of caution and very little left to chance.

Of course, OPSEC scenarios may not make sense in day-to-day proceedings, where maximum privacy is not really required. However, having OPSEC knowledge helps in the same way it helps to know how to change a tire. You don't need to do it every day but, in the rare case that your tyre gets punctured on a highway and leaves you stranded, you should know how to do it yourself.

I mean, you can't always rely on the possibility that a Good Samaritan is going to appear out of nowhere to come and help, can you?

---

[1] You cannot buy a mobile connection without proper documentation (e.g. Know Your Customer, or KYC) in many countries. Buying it in someone else's name is absolutely NOT recommended!

Chapter 14

Epilogue

Introduction

You have now reached the end of the book. Congratulations!

If you made it this far AND also followed my recommendations along the way - well done!

Let's take a quick look at how your efforts have shaped up, shall we? Here's the same QR code that you scanned in the first chapter. Bring out your smartphone, scan it (again) and open the link that appears on the screen.

[QR Code: https://leaktest.privacy.clinic]

Do the results look any different from what you saw the first time?

If you didn't follow any recommendations in the devices section, you are not going to see any change in the analysis. Try going back to the chapters on smartphones and following the recommendations, maybe?

If you did follow my recommendations, they should. If you never went beyond the BASIC recommendations, you are unlikely to see much change in your results, since the BASIC recommendations were mostly about providing you with relevant information and equipping you with knowledge.

Of course, I am not saying you must follow only the EXPERT recommendations -- it wouldn't be a very smart thing to do, and it is guaranteed to throw your daily routines completely off-track!

I mean, can you imagine living your life without Google Maps? Or even Windows 10, in some cases? Sure, there are several alternatives for those services, but I don't want you to adopt those alternatives just because I tell you to -- certainly not at the cost of making your life difficult [1] . I want you to make an informed choice based on the information presented to you in this book.

Throughout this book, I have attempted to show you how these services might leak your private information. I have tried to teach you the different ways to stop that from happening, or alternatives if you can't stop that from happening. It is entirely up to you to make an informed decision about what works best for you from a cost-benefit analysis perspective.

Anyway, let's analyze your scores and try to understand how exactly (and how much) following all those recommendations haveimpacted your privacy.

Updated analysis

If you have been keeping a score of the various recommendations you followed through the book, now is the time to tally all of them and get a final score.

If you scored:

0 - 50 points, then you are a “Novice.”

51 - 100 points, then you are an “Amateur.”

101 - 150 points, then you are a “Pro.”

151 - 200 points, then you are a “Legend.”

What do these titles mean?

The Novice: You probably earned this title because you chose to follow mostly the BASIC recommendations. Now, there's nothing wrong in that, but this basically tells me that you either like keeping yourself informed or you are afraid to take the next step [2] .

Well, now would be a good time to revisit all those recommendations and take the next step, I guess. You already have the information, why not act on it?

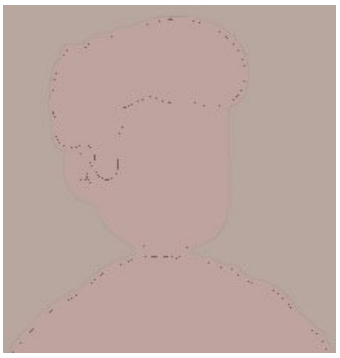
The Amateur: You didn't want to risk following any of the ADVANCED recommendations, correct? You essentially stopped yourself from attempting the ADVANCED recommendations because you were afraid you might end up accidentally breaking something. Well, you won't know until you try, will you?

Look, I'm not saying you should go back and break something. I'm saying if you don't break it, how will you learn how to fix it?

The Pro: Ah, the intrepid explorer! You like tweaking things and changing things, and getting your hands dirty, don't you? You like pulling out the guts and examining them closely to see if they reveal any secrets, don't you? I bet your favorite part of watching crime shows is when the forensic analyst comes on screen!

I'm just kidding. It is good to see you make an attempt to actively try and change the status quo instituted by Big Tech. I'm proud of you, carry on!

The Legend: Hey there! Glad to make your acquaintance! I hope you liked this book. Do let me know your honest thoughts -- my contact details are floating somewhere on the internet. If you do find them, give me a call on the first Saturday of any month, between 5 PM and 6 PM. I'd like to involve you in my next project.



Something tells me you are going to love it. ;-)

Conclusion

Imagine, for a moment, the life of Harry Truman, the unwitting star in the fictional universe of The Truman Show . His life was a carefully constructed series of events in which he had no active role to play but which definitely played an important part in his development. Everyone around Harry was in on the secret, but no one was allowed to tell him. His life was a carefully constructed facade, beamed live to millions of viewers, while he continued to exist in blissful ignorance.

If you were in Harry Truman's shoes, would such a life be truly representative of the real you? If most of your decisions were a result of choices that were severely limited, were the decisions truly decisions in the first place? Would they even be valid?

The reason I am talking about The Truman Show is thatit is a surprisingly good analogy to what we've been discussing through this book.

You are Harry Truman in this scenario. The domed studio shown in the movie is the internet. The people around Harry Truman are the companies tracking your information on the internet. Their behaviors are the ads that you see on the internet and Harry's likes and dislikes determine whether the behaviors reappear or disappear from his life.

For a large part of the movie, Harry does not get to make a 'real' decision about any part of his life. He merely gets to choose from a severely limited set of options presented to him as fait accompli.

Don't you think the whole thing is a pretty good metaphor for the internet and privacy on the internet?

That's also why I decided to write this book. I believe your personal data should be afforded the same rights as your body -- no one should be allowed to take advantage of it, certainly not without your consent, and the consequences of violating your trust should be severe.

Sadly, the people who were supposed to ensure that our personal rights did not get violated did not pay much heed to things as they were developing. It has now reached a point where privacy on the internet is (mostly) a myth. In fact, any discussions about the right to privacy on the internet are summarily dismissed either as pipe-dreams or as a hipster rebellion . It is sad that this current state of affairs has become the new normal.

Privacy is not a pipe-dream; it is a fundamental right. It is high time we decided to have a coherent and mature discussion around the subject. I am glad you chose to join me in having this discussion. Now, I urge you to have this discussion with someone else.

I'll leave you with these words from the movie, The Laundromat:

Privacy and secrecy are two different things. Privacy is locking the bathroom door when you want to take a pee. Secrecy, on the other hand, is locking the door because what you are doing in a bathroom is not what people usually do.

What we do behind closed doors should be nobody else's business anyway, no?

---

[1] No matter how much Windows disrespects the privacy of your personal data, using Linux is sometimes just NOT an option, you know? *cough* gaming *cough*

[2] There is also a distinct possibility that you were selective in scoring the points or that you didn’t score yourself in some chapters.

Chapter 15

Bonus Chapter: Useful Tips and Tricks

The 10 Android permissions listed under “dangerous” protection level.

At the time of writing this book, there were 10 permission groups classified under the dangerous protection level that could be toggled on/off for various apps.

In this appendix, I've listed the category of apps that typically use these permissions and apps that *atypically* use them. Atypical usage refers to usage that is not immediately intuitive. For example, some banking apps and shopping apps will often request SMS permission to read OTP messages from the SMS inbox directly.

In this appendix, I've also presented potential risk profiles for each permission and described the hypothetical scenario(s) in which these permissions may be misused.

Body sensors: This permission allows an application to access data from sensors that the user uses to measure what is happening inside his/her body, such as heart rate.

Typical usage: Fitness apps, companion apps for fitness wearables.

Atypical usage: Calorie counting apps.

Risks: Information about your health can be shared with malicious apps, which might share/sell it to other malicious third-parties.

Calendar: This permission group allows an application to read and write the user's calendar data, that is, create/update and display calendar entries made by the user.

Typical usage: Calendar apps, meeting apps, and more.

Atypical usage : Banking apps, email apps, GTD apps, and more.

Risks: A malicious app can share the details of your personal calendar with third-parties which may include people interested in your whereabouts.

Call logs: This permission group allows an application to read and write to the user's call log, that is, create/update, and display calls made and received made by the user.

Typical usage: Dialer apps, launcher apps.

Atypical usage: Apps like TrueCaller use this permission to provide 'global' caller identification services.

Risks: Malicious apps can upload your call history to their servers and sell it to other malicious third-parties.

Camera: This permission allows an application to access the camera device.

Typical usage: Camera apps, photo apps, social networking apps, scanner apps, and more.

Atypical usage: Banking apps, shopping apps, MFA apps, browsers, and more.

Risks: Malicious apps having access to your camera could secretly turn it on and record your activities.

Contacts: This permission allows an application to read and write to your contact list, that is, create/update and display contacts stored in your phonebook, on your device. It also allows applications to access the list of accounts (for example, WhatsApp, Facebook, Instagram, Twitter, and more.) used on your device.

Typical usage: Dialer apps, social networking apps, email apps, and more.

Atypical usage: Calendar apps, shopping apps, ride-sharing apps, messenger apps, banking apps, and more.

Risks: Malicious apps with access to your contacts can share/sell your address book data with other malicious third-parties who can then use the data to spam, phish, scam, or do any number of similar illegal activities.

Location: This permission group allows an application to access approximate and/or precise location, that is, identify where you are based on the cellular networks in your area or by using the GPS sensor to identify your exact location.

Typical usage: Maps app, ride-sharing apps, delivery apps, camera apps, and more.

Atypical usage: Companion apps to wearables and IoT-enabled devices, shopping apps, social networking apps, and more.

Risks: Malicious apps can track your location to build a profile of your daily habits and frequently-visited locations. Photos and/or social media updates with geotags embedded in them can be used to identify your home and/or work address. There have been instances of robbers targeting homes of users who have posted on social media about being out on vacations.

Microphone: This permission allows an application to record audio. Typically combined with the camera permission, it allows users to record videos with sound.

Typical usage: Camera apps, music recognition apps, dictation apps, voice assistant apps, and more.

Atypical usage: Speech-to-text apps, home-automation companion apps, keyboard apps, note/memo apps, even WhatsApp and more.

Risks: Apps that respond to keywords are quite popular among people but, for them to work, they need to be listening to ALL the time. This means your audio is constantly recorded and evaluated, and not always at device-level. Sometimes, audio may be sent to remote servers for processing, where there could be potential for malicious actors to intercept private communications.

SMS: This permission group allows an application to read, write, and send SMS text messages, receive WAP push messages, and receive MMS messages

Typical usage: Messaging apps, communication apps, and more.

Atypical usage: Banking apps, shopping apps, ride-sharing apps, and more.

Risks: Some apps request this permission to auto-read OTP messages and save you the trouble of entering it manually. However, malicious apps can use this permission to automatically subscribe you to unwanted paid services, or send messages to premium numbers, or spam people in your contact list.

Storage: This permission is the most commonly requested permission, and it allows an application to read and write to the external storage on your phone. Unlike internal storage, external storage is NOT sandboxed; that is, apps writing to the external storage on your phone can also READ other folders in your external storage. Granting this permission to an app typically implies that you are comfortable with the app accessing the various folders in your external storage.

Typical usage: Most apps

Atypical usage: Most apps

Risks: Apps that have been granted permission to read and write to external storage have the ability to read, change, and delete ANY file in your external storage. A malicious app could easily run specific commands to delete ALL the files in your external storage.

Telephone: This permission allows an application to read the state of the device, that is, the phone number of the device, current network information, the status of ongoing calls, and a list of accounts registered to the device. Apps granted this permission can make/answer/redirect calls, use VoIP, among other things

Typical usage: Dialer apps, launcher apps, call recorder apps, and more.

Atypical usage: Banking apps, shopping apps, messaging apps, and more.

Risks: Malicious apps can spy on your phone calls, track incoming and outgoing numbers, and even make calls to premium numbers without your consent.

How to setup your Android without Google Services

Google Mobile Services, while they may seem tightly-coupled with the Android OS, are not entirely necessary for Android OS to function. There is an entire ecosystem of apps and services designed to allow you to operate an Android phone without requiring Google services.

This, however, requires a fair bit of technical know-how and I recommend that you continue along this path if and only if:

You have experience with installing anOS on computers and phones.

You have either flashed or rooted Android phone (or jailbroken an iPhone) at least ONCE in your life.

You have a clear idea of the various ways in which tinkering with your phone can go horribly wrong.

You agree that you and YOU alone will be responsible for whatever happens to your device if you follow any suggestions outlined from here on.

Since you are still reading, I will assume that you said yes to all of the conditions above. If not, skip to the next section NOW!!

There are multiple tutorials available on the internet, and I strongly recommend that you search for one that is suitable for your phone model and follow along closely. Due to the speed and frequency of updates to both phone hardware and software, the information that is presented in this book is likely to be at least a little bit obsolete by the time it reaches you. The overall process is likely to be the same, but the specific steps are

likely to be different for different phone models at different times.

Having said that, here's what you'll need to do to use Android without any of Google's services:

Identify a suitable custom ROM

Okay, first things first, you will need to figure out if a suitable custom ROM is available for your phone model. Typically, Lineage OS (previously known as CyanogenMod) or some version of AOSP (Android Open Source Project) should be available for your specific phone model. If you don't find your phone model on this list, I strongly recommend that you abort this attempt and head straight to the next section, NOW!!

Prepare your phone

Important!!

WARNING!! Be very, VERY careful of what you do here. This part is a bit tricky, and it could brick your phone, that is, render it into a very expensive paperweight. Consider yourself warned!

You will need to unlock your bootloader and flash a custom recovery on your phone. The steps involved in this process are quite intricate and involve using specific commands to unlock the bootloader. Also, unlocking the bootloader may void the warranty of your device, so please be absolutely sure that you *want* to do this.

Look up your phone model on Google and see if you can find a detailed step-by-step description of the process. Head over to XDA if you can't find your phone model on Google - they may have unofficial ROMs that might be suitable for your phone. Usually, the forum post will also have the corresponding instructions on unlocking your bootloader and flashing a recovery.

Again, if you don't find them even on XDA, I strongly recommend that you abort the process immediately.

Boot into the recovery mode and MAKE A BACKUP!!

This is, without doubt, the MOST important step because flashing a custom ROM requires completely wiping your device. You will lose ALL of your data, and I mean ALL your data -- downloads, Bluetooth transfers, apps you may have installed, settings you have changed, documents, games -- every single thing!

Typically, the most common recovery tools include a backup option that will allow you to, well backup everything on your phone. Alternatively, you could use third-party software such as Titanium Backup Pro, or NANDroid to make a complete backup of your phone in case things don't work out the way you plan.

Remember, however, that these backups are often quite large, so you might need to make space in your phone storage to ensure that the backup goes off without a hitch. This is a necessary step in case something goes wrong while installing the custom ROM and you have to revert to previous settings.

Download MicroG instead of GApps

Most Custom ROMs are AOSP-based and, as a result, they do not include the core Google apps and services. However, many third-party apps rely on the Google Play Services framework to run correctly on Android.

MicroG bridges this gap by providing a pathway to install these necessary services on your device but without the use of Google and their default environment.

For more details, you can refer to the excellent guide on GadgetHack titled, Use Android Without Any Google Apps or Services, found here:

https://android.gadgethacks.com/how-to/use-android-without-any-google-apps-services-0193735/

Scan the QR code shown alongside to open the link in your browser.

Wipe your System and install the custom ROM

I will refrain from giving any generic instructions in this section because there is no one-size-fits-all when it comes to installing a custom ROM. You'll have to search the internet for a post or a (tutorial) video that deals specifically with installing a custom ROM on your device and follow the instructions to the letter.

In fact, I strongly recommend that you follow the instructions exactly as written/shown to minimize any chances of bricking your phone. Just make sure that you *don't* wipe your internal storage or you will be left without any OS on your phone, that is, you'll end up bricking your phone!

If you did everything right, you should be able to boot your phone into the custom ROM of your choice! Enjoy your shiny new custom ROM!

Useful apps that you should definitely consider installing

By now, you must have realized that the inherent insecurity of smartphones makes the idea of privacy a difficult one to maintain - especially when it comes to Android phones. Despite the best efforts of manufacturers and the engineers at Android, the availability of millions of apps in the Google Play Store means that the chances of finding malware are much higher than normal.

Therefore, there are certain kinds of apps that, we think, are an absolute must for every smartphone – both Android and iPhone. We'll try and cover as many apps as we can in the subsequent sections. However, this list is neither exclusive nor exhaustive. That is, not all apps that appear on this list are absolutely necessary, and this list does not list ALL the necessary apps. Also, we are not affiliated with any of these apps, but we can certainly vouch for them based on our research and knowledge of the subject.

That said, you can always refer to the latest, most updated list of these apps over at the companion website to this book, that is, privacy.clinic. Scan the QR code given alongside this paragraph to open the relevant page on your phone, right now.

[QR code links to https://privacy.clinic/privacy-related-apps-for-your-smartphone]

Password managers

What: Password managers take away the hassle of remembering passwords for various sites and services by providing a secure vault to store all your passwords.

Why: Most users regularly reuse their passwords -- a practice I do NOT recommend. If the password you re-use were to get leaked, all of your logins immediately become vulnerable.

How: Using a password manager allows you to set complex passwords without having to remember them – the password manager service does the remembering for you. You can use the built-in random password generator to set an absurdly long password, filled with special characters.

I strongly recommend changing all your passwords to lengths of 20 characters or more wherever possible, as soon as possible.

Popular options: Lastpass, 1Password, Dashlane, and KeePassXC

Authenticators

What: Multifactor authentication (MFA) is an additional layer of security for your devices and services. The most commonly known form of MFA is two-factor authentication, (2FA) which is available with most of the popular services on the internet.

Why: The advantage of having 2FA enabled on your device/service is that, even if your password were to be leaked somehow, an attacker wouldn't be able to gain entry into your device/service without the correct OTP which can only be accessed using one of these apps, or by accessing your text messages or answering the OTP call on your phone.

How: When you turn on 2FA for a device or a service, you need to enter an additional one-time-password (OTP) along with your regular username and password to completely access the service. This OTP can be generated on your device using one of these Authenticator apps called TOTP, or time-based OTP or gets sent to your phone via text message (SMS) or a phone call.

Popular options: Authy, Google Authenticator, and Azure Authenticator.

Ad blockers

What: Ad blockers are a fairly recent addition to the internet, and they do exactly what the name says -- they block (most) ads from appearing on

your device screens. Think of it as having a doorman sitting outside your frontdoor, who screens all incoming guests and prevents unwanted guests from entering your house without your explicit permission.

Why: I understand that ads are a way for content creators to make money on the internet. However, many ad networks indulge in pervasive and intrusive tracking of the user, which is something I cannot endorse in good conscience. Moreover, the risk of malware infecting your phone due to misleading ads is also quite high. That's why I strongly recommend using adblockers on your device.

How: Ad-blockers route your internet requests through a locally installed VPN on your device. The requests are then compared against curated lists of known adservers and blocked when a match is found.

Popular options: Blokada and AdAway

VPN

What: VPNs are secure connections to another network over the internet. A securely encrypted VPN also prevents malicious actors from sniffing your internet activity and exposing your private details.

Why: VPNs are extremely useful when it comes to bypassing online censorship imposed by authoritarian governments, evading nosy ISPs, or just generally any entity looking to block your digital experiences. VPNs allow you to access geo-restricted content by bypassing IP-address based filters used by such websites.

How: VPNs change your public-facing IP address to that of the VPN, allowing you some degree of privacy and anonymity.

Popular options: ProtonVPN, Private Internet Access, ExpressVPN, and Nord VPN. Expert users may even want to setup their own VPN server.

Privacy-aware search engines

What: A privacy-aware search engine, much like the default Google app, provides useful search results for your chosen keywords but it respects your privacy by not sending/storing additional meta-data every time you conduct a search.

Why: The default Google app is designed to collect a ton of data and store it on Google's servers. This data is analyzed by Google to provide you with highly personalized suggestions and recommendations. However, research has shown that too much personalization results in users being trapped in a filter bubble; that is, only the information that is palatable to users gets greater visibility.

How: Using a privacy-aware search engine helps circumvent the filter-bubble since your searches and activities are not tracked for personalization. Privacy-aware search engines, therefore, are helpful in making the user aware of multiple options and alternatives.

Popular options: DuckDuckGo, Startpage, Qwant, and more.

Secure instant messaging apps

What: Secure instant messaging apps use end-to-end encryption to ensure that the message being sent can only be read by the intended receiver of the message. If the message were to be intercepted, it would remain unreadable, since the only person with the proper decryption key is the intended receiver.

Why: In 2013, it was revealed that the NSA (National Security Agency, USA) was collecting hundreds of millions email and instant messaging contacts directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple. Soon after, in 2014, the Electronic Frontier Foundation (https://eff.org) released their instant messenger security scorecard, which gave a perfect score to only 7 out of 39 messaging apps available at the time.

How: Secure instant messaging apps employ end-to-end encryption, that is, the message gets encrypted on your device with a key that is only available with the intended recipient.

Popular options: Signal, Wire, Telegram, and Wickr.

Private browsers

What: Private browsers are browsers designed to keep your personal information safe by utilizing highly-secure end-to-end encryption.

Why: The default Browser app on your Android smartphone or the Google Chrome browser can be quite intrusive since they are designed to collect tons of data about your browsing habits. I strongly recommend using private browsing, because browsers are meant to share details of the internet with you, and not vice-versa!

How: Judging by the amount of data your browser shares with various third-parties, one could say that modern browsers share more similarities with two-way mirrors than windows. Pairing a good private browser with a good, privacy-aware VPN significantly decreases your identity footprint

and may help render you (somewhat) anonymous, too.

Popular options: Firefox Focus, Tor Browser, Brave, Epic, and more.

App locker

What: Most modern phones provide an app locking feature that inserts an additional lock screen before the app is available for you to use. Users must unlock this additional lock-screen before continuing to the app.

Why: If an adversary gains access to your phone, they should not be able to access any of these apps easily. It needs the ability to prevent direct access to any apps that contain sensitive data, such as banking apps, gallery apps, and note-taking apps, password managers, and more.

How: Check if your phone has an in-built app-locking feature by opening Setting and scrolling down to There are third-party apps that perform this function quite securely, and you might want to look into that option as well.

Popular options: AppLock by Norton, Applocker by DoMobile, and more.

Alternative app stores

An App Store, as the name suggests, is a repository where you can search for and download apps for your smartphone. Typically, for iPhone users, this would refer to the App Store and for most Android users; this could refer to the Play Store.

I say most Android users because, unlike Apple iOS, Android allows for the possibility of using different repositories for sourcing and installing your apps. Apple does not. If you want to sideload even a single app on your iPhone; you'd have to jailbreak it first.

There are several reasons why you might want to install an alternative app store. Some of the main incentives are:

Free apps: Some alternative app stores run frequent promotions and deals where certain premium apps are heavily discounted or made free from time-to-time.

Recommendations and curations: Alternative app stores have their own recommendation engines, which could result in you discovering different apps. Some alternative app stores may also occasionally (or frequently) post curated lists of apps.

Localization: Some alternative app stores are localized to cater to a specific category or people, for example, a specific country.

However, alternative app stores are also fraught with a lot of risks, since their security policies may not be as rigorous as Google and the Android Play Store. There may be a significant risk that your phone might get infected with malware from a shady app in one of these alternative app stores.

For Android

For example, some phone manufacturers like Xiaomi even have their own App Store, where users can download and install additional manufacturer-branded apps for their smartphones. However, apps from one store are usually not installable/usable on phones made by other manufacturers, but you'll have to check that.

That said, there do exist several full-fledged alternatives to the Google Play Store that provide similar functionality. Some of the notable ones are:

Amazon App Store: Developed by Amazon, it offers close to half a million apps (both free and paid) that you can download and install on your Android device.

F-Droid: A community-run, free software project, F-Droid is developed by a wide range of contributors and only hosts apps that qualify as FOSS (Free and Open-Source Software) .

Samsung Galaxy Apps: Initially developed by Samsung as a collection of companion apps for the Samsung Galaxy series of phones, it was recently opened to all developers.

A quick search on Google will reveal many more app stores catering to different niches; for example, the AppsLib store was designed as a store for tablets but didn't seem to have gained much traction. Aptoide is another independent app store that provides the ability for developers and manufacturers to create their own app stores for their users. There are a bunch of browser-based app-stores as well such as SlideME, GetJar, and more.

One thing to note is that you won't find any of these app stores on Google Play Store. Instead, you'll have to open the web page in a browser, download the installation file (usually a .apk file) if it is available, and install it manually on your Android device.

For Apple

Like I said earlier, Apple does not allow for the installation of apps that aren't downloaded from the official App Store -- not even sideloading. There are a few alternative app stores available for the Apple iPhone. However, these aren't truly independent and app stores, that is, they have basically curated app repositories running with an exclusive enterprise license granted by Apple. You may find good promotions, deals, and discounts on some apps but, overall, the apps they carry are the same as the ones available on the Apple App Store.

You will need to jailbreak your iPhone if you want to truly slideload apps on your iPhone. For jailbroken iPhones, Cydia is the go-to App Store, and it is automatically installed when you jailbreak your iPhone.

You can add multiple source-repositories in Cydia, but be careful, as adding a malicious repository could potentially infect your jailbroken iPhone with malware.

Conclusion

Apple does not allow installing independent alternative app stores and the only way to use one is to jailbreak your iPhone. I've already explained to you in a previous chapter why that may not exactly be a good idea. Jailbreaking an iPhone is not something you should do as a spur-of-the-moment thing. It is a decision that can have serious consequences and needs to be thoroughly vetted with someone knowledgeable about iPhones before it is done.

For Android, the only alternative app store even worth considering is F-Droid , and I suggest that you definitely give it a go. The apps on F-Droid are free and open-source and, as a result, they usually lack the polish typically seen in the apps available on the Android Play Store. However, what they lack in terms of design, they usually (more than) make up in terms of functionality, security, and privacy.

The other app stores mentioned above are also worth considering but, remember, each new app store is a separate attack vector for malicious actors to propagate their malware. Sure, some of them may have exactly the app you are looking for but, before you install the app, make sure you stop and consider both the inherent risks and ethics of your actions at least once, especially if you are looking to pirate the app. Furthermore, there may be apps on these alternate app stores that may contain malicious code. You might end up completely bricking on your phone just because an app promised you an 'easy hack to win all your 2v2 matches in your favorite battle royale game' and you were naïve enough to believe it.

I would strongly recommend that you stick to the default app stores -- better the devil you know and all that.

Checking your email on an unknown computer

If you ever need to log into your email on an unknown computer, that is, a computer that is not your home computer or work computer, I recommend that you:

Do NOT log in at all.

DO NOT LOG IN AT ALL!!

However, if you absolutely must log in to an unknown computer, follow these steps to ensure maximum privacy and minimize any potential security issues:

Ensure that you have MFA enabled for your email account.

Choose one of the following options:

1) Use a bootable USB to load a secure, live OS such as Tails or Whonix.

2) Install a VM, Use the removable disc option to load an ISO of a live OS and boot it up.

3) Download and install a sandboxing application such as Sandboxie, BufferZone, or similar.

4) Download a portable and/or sandboxed version of your favourite browser, for example, BitBox.

Install the corresponding browser extension for the password manager you use for your email.

Open the private browsing option for your preferred browser and open your email login webpage.

DO NOT TYPE OUT YOUR PASSWORD UNDER ANY CIRCUMSTANCES!

1) Use the password manager extension to log into your email account!

2) Fill out the OTP shown by the authenticator on your device.

While your email is loading in the browser:

1) Log out of the browser extension for the password manager.

2) Uninstall it. Leaving it installed is a much, MUCH bigger security risk.

Do not download any attachments or files, if possible. Instead, forward them to whoever needs it. If you absolutely must download an attachment, remember where you saved it.

After you are done checking your email, SIGN OUT of your email account.

Close the private browsing window. This ensures that any leftover cookies, data, and many more, get deleted.

Depending on what you did in step 2, perform the corresponding reverse procedure, that is, uninstall the sandbox application, or shutdown the VM, or reboot the live OS.

Or,

You know, if you want to save yourself all this hassle, do NOT log in to your email account on an unknown computer.

Your Privacy Score Card

Total Privacy Score: _____ points

Dated: _____

For more information, go to https://privacy.clinic