"A fresh perspective on cyber security"
Melecia McLean, Security Behaviour and Culture Lead, TikTok

HACKED

The secrets behind cyber attacks

Jessica Barker

KoganPage

Praise for *Hacked*

"A must-read. It offers a fresh perspective on cyber security, emphasizing the human element and making it invaluable for anyone interested in safeguarding their digital presence." MELECIA MCLEAN, SECURITY BEHAVIOUR AND CULTURE LEAD, TIKTOK

"*Hacked* is like a dictionary of manageable cyber risk. As always, Barker's writing is warm and accessible, and contains an abundance of common-sense solutions". CIARAN MARTIN, PROFESSOR, UNIVERSITY OF OXFORD AND FORMER HEAD OF UK NATIONAL CYBER SECURITY CENTRE

"Does a great job of demystifying cybe rsecurity. Read this book, and then pass it on to a loved one. We need to protect ourselves and each other." LISA PLAGGEMIER, EXECUTIVE DIRECTOR, NATIONAL CYBER SECURITY ALLIANCE

"Crafted by a cybersecurity visionary, this essential guide tackles the spectrum of cyber threats. It provides actionable strategies and expert insights into safeguarding digital lives against sophisticated scams and vulnerabilities." SURINDER LALL, SVP INFORMATION SECURITY RISK MANAGEMENT, PARAMOUNT

THIS PAGE IS INTENTIONALLY LEFT BLANK

Hacked

The secrets behind cyber attacks

Jessica Barker

Publisher's note
Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and authors cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the editor, the publisher or the author.

First published in Great Britain and the United States in 2024 by Kogan Page Limited

2nd Floor, 45 Gee Street
London
EC1V 3RS
United Kingdom

8 W 38th Street, Suite 902
New York, NY 10018
USA

4737/23 Ansari Road
Daryaganj
New Delhi 110002
India

www.koganpage.com

Kogan Page books are printed on paper from sustainable forests.

ISBNs

Hardback 978 1 3986 1 3720
Paperback 978 1 3986 1 3706
Ebook 978 1 3986 1 3713

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library.

Library of Congress Cataloging-in-Publication Data

***

When I was about 13 years old, I stopped complaining about the noise of the modem long enough for my brother to introduce me to the internet. He described it as a way to 'learn anything about anything'. At that time, I would never have dreamed that my future career would be focused on helping people enjoy the internet safely. Almost three decades later, I dedicate this book to Daniel Barker, my favourite big brother.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Contents

About the author

Jessica Barker MBE PhD is an award-winning leader in the human side of cyber security. She has delivered face-to-face awareness sessions to over 70,000 people and over 80 international keynote speeches including to NATO, the World Government Summit and the RSA Conference. Jessica is the go-to expert for media such as BBC, Sky News and Wired. She serves on numerous boards, including the UK Government Cyber Security Advisory Board. She is the author of the best-selling book *Confident Cyber Security*. In June 2023, Jessica was awarded an MBE for services to cyber security by King Charles in his first Birthday Honours.

Preface

While writing this book, I received an out-of-the-blue email from someone who had watched one of my YouTube videos and wanted to share an experience with me about security, empathy and compassion. James is a business leader in the US. He told me of a time about 25 years ago, when he was in his 20s and was conned out of $15 by a street hustler, in what James described as 'a fast-talking quick-change scheme'. He told me that he went home feeling stupid and told his father, who had been a bank manager for over 30 years, all about the experience. His father broke down the tricks that the scammer had used. His father explained that bank employees are trained to recognize scams and put the brakes on, but even then they can be confused by those kinds of tactics, aimed to bamboozle and deceive. This helped James realize that being conned did not mean he was stupid, but rather showed that the scammer knew what he was doing, clearly with lots of experience. James was able to look at the experience with fresh eyes and analyse the tactics that the con artist had used. Some 25 years later and a board that James was serving on was approached by a man proposing a collaboration. Throughout the course of this man's pitch, James got a familiar sense. He realized that this man was using the same tactics as the con artist all those years ago. He shut the pitch down and, after a little investigation, discovered that the man had a record of fraud.

I'm always grateful to people like James, who share their experiences with me – although I wish no one experienced fraud, scams or cyber attacks. In James' case, his early experience and – importantly – his father's empathic and educational response, helped him see what undoubtedly would have been a much greater fraud many years later. Awareness and empathy can go a long way in helping us learn the secrets of scammers and criminals, and we can use that awareness to be safer and more secure for the rest of our lives. We can also share this knowledge, just like James' father, with empathy and compassion to help those around us be safer, too. In this book, I will be unpeeling some of the layers of cyber attacks, online scams and fraud. I have interviewed many interesting, experienced people while writing this, and you will hear from them throughout the chapters. I am grateful to everyone who has shared their time and expertise with me; it has made the book richer.

I hope this book helps you understand the reality of cyber attacks, and how those behind the attacks operate. When you finish this book, my aim is that you will be more aware of the strategies and tactics of cyber criminals so that you can spot the red flags of social engineering, practice more secure behaviours and help those around you be more secure online, too.

Acknowledgements

I will never forget those who shared their time, experience and expertise for this book, allowing me to interview them and ask questions, bringing new depth to the chapters. Thank you to Hannah Ajala, Ade Clewlow MBE, Pete Cooper, Sandra Estok, Mark Gallagher, Kenneth Geers, Alastair Gray, Ruth Grover, The Grugq, Benedict Hamilton, Mikko Hyppönen, Ciaran Martin, Erhan Temurkan, Geoff White and Alexander Wood.

Thank you to Matt James and the team at Kogan Page for making this book happen, I appreciate your support, patience and professionalism. I am forever grateful to the team at Cygenta for being the secret behind my success. My husband is a constant source of support, encouragement and cups of tea, which I needed more than ever while writing this book. Thank you, FC, for everything we have overcome and achieved in recent years. Of course, I can't imagine what my life would be like if I wasn't lucky enough to have The Best Parents (official title of Sue and Richard Barker). Last but certainly not least, Bubble the cat deserves an honourable mention for her support services.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Introduction: the groups behind cyber attacks

'Hacked!'

You hear it all the time. Headlines shout of the latest breaches. Cyber crime and hacking features heavily in TV shows and movies, as well as the news. Stereotype images of hackers in hoodies, surrounded by green screens of code, are used to attempt to illustrate the intangible world of cyber security. But which threats should we be truly concerned with? What does cyber warfare and artificial intelligence mean for the evolving threat? Most importantly, how can we decipher the signal among the noise and understand how to protect ourselves, our families, our organizations and our communities?

In this book, I will peel back the layers on the most common cyber attacks and threats, exploring what makes the security of the internet so precarious, where we have made progress and what we can all do to enjoy technology while limiting the potential for harm. By the end of this book, you will understand why cyber crime has exploded so ferociously in the last decade or two and you will appreciate that this technical field is deeply human, too.

It is the human nature of cyber security – and the people I meet as part of my work in this industry – which has kept me engrossed by this field for over 13 years. In writing this book, I have interviewed people with so many different perspectives to shine a light on the secrets behind cyber attacks. As you read through the chapters, you will hear from people who are advocating for victims, investigating criminal gangs, fighting fraud and defending countries. You will also read about life on the other side of the coin – what leads someone to commit cyber crime, how an organized criminal gang targets and exploits victims, and what happens when law enforcement catches up with them.

The global cyber security threat does not come from one particular group or type of person. Countries and state-sponsored attackers hack as part of wider, deeper geopolitical tugs of war. Vigilante hacktivists seek to advance ideological purposes and social causes. Have-a-go hackers (often called script kiddies by the cyber security community) flex their muscles, seeking kudos and lols from their friends. But, financially motivated organized criminal gangs are behind the growing threat that most of us face online. Criminals regard the online world as an easier, faster, cheaper, less risky and more financially

rewarding environment to commit crime compared to traditional crime in the physical world. With challenges of attribution, jurisdiction and resources, law enforcement, investigators, defenders and responders are locked in a cat-and-mouse game with ever-evolving adversaries. You will note that I refer to criminals and not 'hackers', despite what the headlines so often say. While some of the criminals are hackers, not all hackers are criminals – not by a long way. Many hackers work ethically and legally in the fight against cyber crime, and many fraudsters profiting from cyber crime are not hackers. As we will explore, the technical barrier to entry for cyber crime has been lowered: a broad and sophisticated ecosystem of Cyber-Crime-as-a-Service exists, meaning criminals can purchase hacking packages and tools without ever needing hacking skills or expertise.

Cyber security issues do not only exist outside our perimeters. Cases of malicious insiders are often as shocking as they are challenging – as you will discover as you read on. Meanwhile, attackers increasingly focus their attention on us, the people using technology, by subverting our trust and exploiting the way we think, work and communicate. Software and systems are often not made with security – and, especially, security usability – in mind.

Nevertheless, we continue to make progress in cyber security, even if it does not always feel like it. In a field whose purpose it is to focus on flaws, it can be easy to miss the wins. To only pay attention to the one time something went wrong, not the 99 times it went right. To look at the here-and-now, the future threats, and not the progress we have made to get us here. This book includes lots of stories

of cyber insecurity. I aim to unpick the complexity and vulnerability of connected technology as clearly as possible. I also aim to highlight the successes that we continue to achieve along the way. If I could have just one wish from this book, it is that you finish it understanding cyber security a little more. I don't want to leave you scared of the reality behind these attacks. Instead, I hope you will be empowered by the practical steps I share as we move through the chapters, not just to pick up some cyber security practices that you perhaps did not have before, but to share some of these with the people around you who could benefit, too. We can all be susceptible to cyber crime and scams. Overconfidence, believing that 'it would never happen to me', is one of the most dangerous thought processes out there, lulling us into a false sense of security. The case studies and statistics in this book are eye-opening, not least for the fact that they are the tip of the iceberg. For a cyber attack or scam to become a statistic, it must first be known and then it must be reported. Many attacks are never reported and so all estimates of the scale of the problem are just an indication of the true challenges we face.

Awareness is the first step towards a better defence. When we understand the problems we face, and how to address them, we are on the path to better security and greater resilience.

CHAPTER ONE

Phishing

Tens of thousands of computers were wiped by cyber criminals. Employees were forced to rely on pen, paper and typewriters as their computers were taken offline. This organization – a global energy company – had been hacked. And it started with phishing. The attackers sent 250 phishing emails to the target company. The phishing emails got through the filters and landed in the in-boxes of 250 people and, of those, 80 clicked the link. In this case, clicking the link didn't do any damage by itself. But the link took those 80 people to a website that prompted them to enter their usernames and passwords for the company systems. Of the 80 people who visited the page, there were 8 who entered their credentials, and the attackers used those 8 sets of credentials to get access to the company network every day for several months. The email filtering systems had not

spotted the phishing emails, so they were able to get through. The pretext in the emails convinced enough people that they were legitimate. Monitoring alerted the cyber security team to unusual IP addresses on the network, but they did not escalate the incident. The attackers were behind the digital perimeter, able to move further across and into the network for the next two months before they launched the attack that took company operations down.

Email phishing

Phishing leads the way when it comes to cyber attacks. Phishing was the number one complaint reported to the FBI Internet Crime Complaint Center (IC3) in 2022.[1] In research which analysed 23.5 billion cyber attack attempts during 2022, the cyber security business Comcast found that 9 out of 10 attempts to breach their customers' networks started with phishing.[2] Since the beginning of 2019, phishing has grown by 150 per cent each year, with the Anti-Phishing Working Group (a not-for-profit and international association of law enforcement, industry and academia) reporting a record number of 4.7 million phishing attacks in 2022.[3]

Phishing is a form of social engineering, where we are manipulated into doing something we wouldn't ordinarily do. Attackers impersonate reputable companies or individuals we trust, and they are generally aiming to trick us into clicking a malicious link, downloading a malicious document, sharing sensitive information (such as personal or financial data), or transferring money.

Email is still the most common form of phishing.[4] It is easy for cyber criminals to gain access to breached datasets of people's email addresses, or to buy them on the dark web. Sending mass phishing emails is easy, quick, scalable and cheap. The criminals often simply play a numbers game, sending out huge numbers of phishing emails and therefore only requiring a small percentage to take the bait. The classic example of a prince from overseas springs to mind, a wealthy individual who contacts us out of the blue and generously wants to share their fortune with us, if we just pay the cost of a small fee to make it happen. As email providers and organizations have upped their defences (for example with better email filtering and awareness-raising focused on email phishing), and we have all become savvier to plain 'old-fashioned' phishing, cyber criminals have evolved their methods.

Research shows that the more obvious forms of phishing have declined, with criminals moving towards more sophisticated levels of social engineering, using pretexting to persuade us.[5] Pretexting is when a criminal creates a fraudulent narrative, a convincing story, to deceive a target. The pretext will enable them to lend false credibility from a trusted figure or organization and will explain why they need you to take the action they want, such as sharing information with them or transferring funds. Targeted phishing emails are often called spear-phishing, and the criminal sending those may have conducted some online reconnaissance, referring to the target by name, perhaps impersonating a colleague, family member, client or supplier, and referencing information that the target might expect to be confidential, thus adding weight to their pretext.

Criminals often exploit current affairs. This was never more evident than when the Covid-19 pandemic began, and Google reportedly blocked 18 million phishing emails on a daily basis in April of 2020 alone.[6] When most of us feel heartbreak, anxiety and sympathy, cyber criminals see opportunity. As well as the Covid-19 crisis, this is the same with national and international environmental disasters and climate emergencies, as well as the outbreak of global conflicts. One day after Russia invaded Ukraine in 2022, cyber criminals started exploiting the crisis with phishing campaigns. The cyber security company, Tessian, found that the number of web domains registered containing 'Ukraine' increased by over 200 per cent, with 77 per cent of those domains appearing to be suspicious.[7] Cyber criminals register domains as part of phishing attacks, for example to host websites which appear to belong to official charities, prompting visitors to those sites to input their personal and financial data as part of 'charity donations'. They use phishing emails and messages, spoofing official email addresses, to push people to visit those sites and when the victim enters their personal or financial data it is used to carry out identity or financial fraud.

When criminals send emails appearing to be from trusted entities, such as charities or banks, they will often spoof the email address. This means that they manipulate the sender email address to make it appear as if it is coming from a different, trusted source. They also compromise email accounts, which may begin with a phishing email itself. For example, if criminals send me a phishing email that pushes me to visit a webpage and enter my credentials, the criminals then have my username and password. If I don't have multi-factor authentication set up, they can

then access my account and send emails to my contacts pretending to be me. Account compromise and spoofing email addresses are methods that criminals have used (and continue to use) to make business email compromise a more costly problem than ransomware.

Business email compromise

It's a form of phishing that hit Facebook and Google for collective losses of $121 million,[8] IT company Ubiquiti for $46.7 million[9] and the charity Save the Children for $1 million[10] – and reports suggest that business email compromise (BEC) just keeps growing. In 2022, the FBI IC3 unit received 21,832 reports of BEC, with losses over $2.7 billion.[11] Between July 2019 and December 2021, the FBI reported a 65 per cent increase in BEC, which has been reported in all 50 states of America and 177 countries, to the tune of $43 billion dollars lost to this crime globally.[12]

BEC uses pretexting to succeed. These are phishing attacks that target organizations, with the attacker impersonating a trusted figure or organization, generally with the aim of stealing money, infecting the systems with malware or deceiving their victims into sharing data, such as usernames and passwords or confidential company data. Some BEC attacks take the form of so-called CEO fraud, in which the criminals spoof or hack into the email of the CEO (or other C-suite member) and email employees with instructions to make a payment via wire transfer or purchase gift cards and reply with the serial numbers. Other cases are classed as invoice fraud, in which criminals compromise or spoof the email account of a finance

employee at an organization and send fake invoices to third parties requesting payment, notifying that their bank details have changed. BEC scams target individuals as well as companies, with house purchases a particularly attractive target to criminals. In a particularly cruel form of the scam, criminals compromise or spoof the email accounts of lawyers, brokers and mortgage lenders, and hijack communications with people in the process of buying homes, tricking them into sending the purchase funds to accounts they control. BEC works by subverting our trust, with scammers posing as trusted entities, and exploiting our human bias, often using authority bias, urgency, flattery and a need for confidentiality to manipulate victims.

BEC is a difficult crime to disrupt, generally involving decentralized crime groups operating in different parts of the world and routing their criminal gains through many layers of money mules in different countries. However, this does not mean that law enforcement never has any success, as Interpol's Operation Delilah shows. In May 2022, Interpol and the Nigerian Police Force announced the arrest of the suspected head of the cyber crime gang SilverTerrier, aka TMT. Interpol had arrested 14 SilverTerrier members before the arrest of the suspected leader at the Murtala Mohammed International Airport in Lagos, Nigeria.

Operational since at least 2015, some reports suggest that SilverTerrier / TMT attacked 500,000 government and private sector organizations in over 150 countries.[13] Palo Alto Networks Unit 42 tracked the activities of the SilverTerrier group and observed them launching 10 Covid-19 themed malware campaigns, using BEC phishing

emails, in just three months from February to April 2020. Unit 42 noted that the group showed little restraint targeting organizations critical to efforts to manage Covid-19, including attacking government healthcare agencies, local and regional governments, and medical publishing firms across the US, Australia, Canada, Italy and the UK.[14]

As we have become more alert to phishing emails, cyber criminals have not only made the emails themselves more targeted and convincing, for example with BEC, but they have also expanded to subverting other forms of communication. In recent years, there has been an increase in phishing over SMS text messages ('smishing'), social media, messaging platforms such as WhatsApp and telephone calls (sometimes called vishing).*

Phishing phone calls

MGM owns over half of the Las Vegas strip and is the largest employer in the state of Nevada, US.[15] The MGM Grand is the largest hotel in the world, with an estimated 70,000 people going through the hotel every day.[16] That is just slightly fewer people than go through Disneyland in Los Angeles every day.[17]

In September 2023, MGM was hacked, affecting more than 30 of their hotels and casinos around the world.

*In general, I prefer not to use the terms vishing and smishing; I find it makes for clearer communication to simply say 'phone phishing' or 'phishing messages' rather than use specific terms that then need to be defined. When QR code phishing started to be called 'quishing', I knew we'd gone too far!

Customers took to social media to report that slot machines were not working, there were issues with room keycards, ATMs were out of order, and they were having difficulties cashing out casino winnings. Guests complained of having to spend hours queuing to check in, of being unable to use credit cards to make payments and of being issued handwritten receipts from the casino. In the first week of the incident, MGM's share price dropped by 6 per cent.[18]

MGM did not provide many public details themselves, other than confirming that they were subject to an attack and, later, that personal data of some customers had been stolen, including names, driver's license numbers, social security numbers and passport numbers. The CEO of MGM stated that there was no evidence that this information had been used for account or identity theft.[19] However, it can take time for such information to be used in further criminal activity (see Chapter 5). In its Securities and Exchange Commission (SEC) filing, MGM reported that they identified the attack and shut down systems to prevent the perpetrators from accessing financial information of customers. They also estimated that they would lose $100 million in profit due to the incident.[20]

It took over 10 days for operations to return to normal. MGM appears to have been the victim of a ransomware attack, and it reportedly began with voice phishing. While MGM did not release any confirmation of this, the hacking group 'Scattered Spider' appear to have claimed the attack and attributed their initial entry to online reconnaissance and social engineering. Reports suggest that they used LinkedIn to find employees of MGM, then called the MGM IT helpdesk impersonating one of those employees

and requesting a password reset.[21] It seems that the group then infected the MGM network with ransomware made by Ransomware-as-a-Service (RaaS) group ALPHV / BlackCat[22] (see Chapter 10 for more on this form of attack and the role of RaaS). They stole and encrypted MGM data and demanded a payment in cryptocurrency, threatening that otherwise they would release the data. It appears that MGM refused to give in to their demands.

Scattered Spider are believed to be in their late teens or early twenties and based in either Europe or the US, meaning their fluent English is perfect for voice phishing calls on companies in Europe or the US. They are known for using social engineering methods, including MFA bombing and SIM swap attacks (see Chapter 2), as well as phishing messages and voice phishing.[23]

Voice phishing attacks on organizations are reported to have increased five times from 2021 to 2022[24] and voice phishing calls, of course, can affect us at home as well as at work. When Amanda Law received a phone call from someone who claimed to work at her bank, the person on the other end of the phone knew so much information about her accounts that she was convinced it was legitimate. He knew her name, her address, her bank account information and accurately told Law how much money she had on her credit card. The caller told her that her account had been compromised by fraudsters working within her bank and so she needed to transfer her funds into Bitcoin to keep them safe, instructing her how to do so. In total she was scammed out of $12,000 CAD and, when she reported the scam to the bank, she was told: 'The individual responsible had access to your financial

information. You are responsible for protecting it under the terms in your agreement. Your request for reimbursement has been declined'.[25] There are multiple ways in which criminals get hold of our personal and financial data, for example when information is leaked in a data breach and sold on the dark web, stolen via malware or abused by a malicious insider at an organization which is privy to customers' personal and financial data.

Caller ID spoofing

In November 2022, an international law enforcement operation took down a website that allowed criminals to impersonate trusted corporations via pre-built spoofing services. Authorities from 10 countries worked together to support the operation, led by the UK's Metropolitan Police. Users of the iSpoof site signed up and paid a fee, which enabled them to anonymously make spoofed telephone calls, send recorded messages and intercept one-time passwords. The site offered a range of numbers that users could spoof, including banks, retail companies and government institutions. iSpoof provided fraudsters with everything they needed to make phishing calls that appeared legitimate, including custom hold music and call centre background sounds so that victims would be more likely to believe the calls were legitimate, all wrapped up in a user-friendly dashboard for the fraudster to easily conduct their crimes.

There were 59,000 registered users of the site, who paid a monthly fee using Bitcoin, equivalent to hundreds or

thousands per month depending on the different package of features that they signed up for. iSpoof was marketed via a Telegram channel called iSpoof Club, which offered administrative support and promoted the service with a one-minute advert that was as bizarre as it was brazen. The animated video is like something a legitimate company would use to sell their services (perhaps with a limited marketing budget). Professional-looking, happy characters appear on screen as the voice-over exclaims 'iSpoof is here to help!', 'all the tools a spoofer would ever need', 'made by spoofers, for spoofers', before ending 'for the people who love spoofing', while the animated characters celebrate on screen as bank notes rain down on them.[26]

The international investigation into iSpoof found that the site made EUR 3.7 million in less than a year and a half, with UK victim losses estimated to be at £43 million and worldwide losses estimated at £100 million (over $120 million). The website was taken offline, and servers were seized, following the arrest of the site's 'mastermind' and main administrator, Tejay Fletcher, on 6th November 2022 in London. He is believed to have made almost £2 million in profit from running the site and on 18 May 2023 he was sentenced to over 13 years in prison after pleading guilty.[27] Fletcher used the money he made to rent an expensive London apartment as well as buying a Lamborghini, two Range Rovers, jewellery and an £11,000 Rolex. The police investigation, named Operation Elaborate, is the biggest anti-fraud operation ever run in the UK to date. The total number of victims is thought to be around 200,000 globally and 10 million fraudulent calls were made via iSpoof: 40 per cent were in the US,

35 per cent were in the UK and the rest were spread around the world.[28] In the UK, iSpoof was linked to almost 5,000 Action Fraud reports, with an average loss of £10,000 each; one victim lost £3 million.[29]

UK police texted 70,000 people who they believed may have been made a victim of fraud by criminals using iSpoof, in the hope of gathering more evidence and making more arrests. The police communicated that they would only text people on the day of their press release (24 November 2022) and the following day, and that if anyone receives a text from the Met Police about iSpoof outside of those dates, it is likely a scam piggybacking on their activity.[30] When they took down the iSpoof operation, the Metropolitan Police also uploaded their own video to the iSpoof Club Telegram channel. In a genius piece of satire, the police video mimics and mocks the marketing video that Fletcher had previously used on the channel to sell the service. With the same cartoon animation and a similar voiceover to the original one, the police video exclaims 'use our service to tell worldwide police that you are a criminal!', 'all the evidence the police would ever need', 'iSpoof was made by criminals for criminals' before ending 'you made a bad call, the police will be seeing you soon' as the main animated character can be seen – no longer smiling and behind bars.[31] To date, 169 people have been arrested in connection with the website.[32]

Phone spoofing is when a criminal manipulates caller ID to make it look like they are calling from a legitimate, trusted source. It was a core component of Alexander Wood's fraudulent activity (more details on this in Chapter 5) in which he called businesses and impersonated

their bank to convince them to make payments to bank accounts that he and his associates controlled. Spoofing banks and financial institutions in this way is a common spoofing scam. Criminals will often pretend to be from the tax authority of the call receiver's country, such as the IRS in the US or HMRC in the UK, and the caller will often threaten legal action unless a payment is made. Another common spoofing scam is the caller pretending to be technical support, for example from Microsoft or Apple, claiming there is a problem with the receiver's computer, and they need remote access to fix it. When the receiver follows the caller's instructions and sets up remote access, the caller uses this to install malware and steal personal and financial information. Other common spoofing scams include the caller pretending to be from a utility, threatening to shut off gas or electricity unless a payment is made, or impersonating a charity, often using current affairs to ask for a donation. When the criminals have manipulated their victims into sharing personal or financial information, they use this to take more fraudulent payments or commit identity fraud.

When using spoofed caller ID, criminals will most commonly rely on robocalls, which use an automated system to play a pre-recorded piece of audio. For example, this message may say 'you need to renew your auto warranty' and prompt the call recipient to press a button which would connect them with a scammer who then takes over. In 2021, auto warranty scam calls hit 13 billion, accounting for one-fifth of all robocalls made by scammers. In July 2022, the Federal Communications Commission (FCC) in the US took a series of actions which made a big

dent in this scam, which represented the biggest robocall scam in the country. The FCC identified the operatives behind over 8 billion auto warranty robocalls in the US every year – Roy Cox Jr, Arron Michael Jones, their companies and international associates – and forced the eight carriers that Cox Jr and Jones used to stop permitting the traffic. Within a few weeks, Americans received 43 per cent fewer robocalls than they had in the month previous, with the percentage dropping a further 40 per cent the following month.[33] In May 2023, the FCC reported further gains on dismantling robocalls, reporting that their actions disrupting auto warranty scam calls led to a 99 per cent reduction in the robocalls, and they had also achieved an 88 per cent month-to-month drop in student loan scam robocalls.[34]

These are not the only steps the FCC has taken to disrupt scam phone calls in the US. In March 2020, the FCC issued a mandate to telecom companies in a bid to crack down on phone spoofing, demanding that they implement a series of protocols called STIR/SHAKEN. STIR/SHAKEN is a practical mechanism that enables telecom providers to digitally sign and verify numbers, meaning that US consumers could be assured that the numbers calling them are legitimate. However, the rollout of this mechanism has been delayed and extended, meaning that only approximately 25 per cent of all calls in the US are signed.[35]

Unfortunately, although STIR/SHAKEN has the potential to make scam phone calls easier to spot, it will not apply to text messages, which means that criminals are turning more attention to phishing messages. Once again,

the cat-and-mouse game continues. As our defences in one area improve, criminals continue to evolve their tactics.

Phishing messages

Social engineering via fraudulent messages is generally aimed at tricking people into downloading malware, sharing personal or financial information, or sending money to criminals. Romance scams and investment fraud often begin with phishing messages over text, online forums, messaging apps or social media.

Data suggests that phishing texts have increased in recent years, with reports of phishing texts in more than three-quarters of organizations in 2022.[36] In the US, the Federal Trade Commission reported losses of $330 million in 2022, due to phishing texts (double the losses from 2021 and five times from 2018), which is accepted to be a fraction of the problem due to underreporting.[37]

In May 2023, Spanish police arrested 40 people who they allege made over $700,000 as part of a serious organized crime gang (called Trinitarios) that relied on phishing texts to commit bank fraud. Those arrested were accused of sending SMS phishing messages to victims pretending to be their bank, pushing them to click a link to resolve a supposed security issue. When the victims clicked the link, they were taken to a spoofed banking website where they were prompted to enter their usernames and passwords, which the criminals used to log in to their bank accounts and commit fraud, requesting loans and purchasing cryptocurrency. A list of 300,000 phishing victims was

discovered at the time of arrest, along with information about the gang's organizational structure. The group was said to be using an extensive network of money mules and sending money to foreign bank accounts, used to purchase real estate in the Dominican Republic. It is believed they defrauded 300,000 victims.[38]

When criminals find a form of social engineering that works for them, they will double-down on it, following trends and numbers – we see this with ransomware (see Chapter 10), business email compromise and QR phishing.

QR code phishing

The Covid-19 pandemic – and our response to it – was heavily exploited by cyber criminals. As this chapter has already explored, cyber criminals wasted no time in using Covid-19 in phishing campaigns, exploiting our anxiety, combined with our need for information in a constantly shifting landscape. The forced digital transformation that many organizations quickly implemented, such as increased cloud implementation and new working from home infrastructure, often inadvertently left new avenues for cyber criminals to exploit.

Another technology which cyber criminals are increasingly exploiting is quick-release codes, more commonly known as QR codes. A more common sight since the start of the pandemic, QR codes are small barcodes that smartphone cameras read, which then generates a web link, prompts the download of an app or file or directs a

payment. In January 2022, the FBI warned of the rise in QR code phishing.[39]

Unfortunately, this warning did not help a 60-year-old woman in Singapore who was scammed out of $20,000 in a case of QR phishing. The victim visited a bubble tea store and was pleased to see a sticker on the door, offering a free cup of milk tea in return for scanning the QR code and completing a survey. When she scanned the code, an app was downloaded onto her Android phone, purportedly so she could complete the survey, but in reality, the malicious app was used to steal $20,000 from her internet bank account.[40]

Hybrid phishing

Phishing messages can reach us in a variety of ways: via increasingly sophisticated emails, text messages, social media, and messaging platforms such as WhatsApp. It is also important to understand that multiple communication channels can be used, and these are the most convincing of all attacks.

As we have improved our defences against phishing – both in terms of greater awareness and better technical controls keeping phishing emails, in particular, at bay – criminals have realized that sending an email or message prompting the victim to call them is one way to evade those defences. PayPal payment requests are one sneaky form of hybrid phishing. Criminals use legitimate PayPal accounts to send targets money requests – which are also a legitimate feature of PayPal. They send a large number of

these out to random PayPal accounts, relying on a spray-and-pray approach. They make it look to the recipient as if the payment is for a genuine product or service, but it is a bogus purchase – one that the recipient never made. If the recipient pays the money request, the criminals will be happy. But they know that lots of people will realize they did not make the purchase. So, the criminals include a number for the recipient to call if they do not think the payment is legitimate. They are relying on people making that call, where they trick the caller into sharing personal and financial data, for example by posing as PayPal's fraud department.

Criminals do not just stick to one form of phishing, but increasingly use multiple methods to manipulate us. This was the case with the cyber crime group that Spain's National Police disrupted in October 2023, when they arrested 34 criminals who they allege were responsible for phishing campaigns over email, voicemail and SMS texts. Upon their arrest, police seized two simulated firearms, a katana sword, $84,736 in cash, luxury vehicles and a database of personal information belonging to four million people. Over 1,000 complaints had been filed about their scams, with over $3 million stolen from victims.[41]

It is an unfortunate reality of cyber crime that, as we evolve our defences, criminals morph their tactics to find their way around our controls. As time moves on, we will see more hybrid phishing, more phishing beyond email and we can expect to see more use of artificial intelligence in phishing campaigns which – as covered in the AI chapter – has already begun. Hybrid phishing is increasingly being used in business email compromise; for example,

with the fraudsters making a phone call to warm up their victim, building rapport and trust, before sending a phishing email confirming the fund transfer request. Adding in AI abilities, for example with deepfake voice imitations, only makes this more convincing.

However, there are effective steps we can all take to guard against phishing. Our best defence starts with being aware of how cyber criminals operate and the fundamental behaviours we can practice to stop them in their tracks.

Protect against phishing

The common advice against phishing is to look for spelling and grammatical errors, hover over links to ensure they look as expected and check the sender's email address to make sure the email really is coming from the person it claims to be. This advice can still be helpful in some instances, but it is not 100 per cent. Fraudsters don't always have bad English-writing skills and, those that do now have large language models (LLMs), such as ChatGPT, to do the heavy lifting (see Chapter 14). Email accounts can be compromised or spoofed so the email address can look valid even when it is not. Some phishing emails, such as the PayPal payment request scam, take advantage of legitimate online services to have a veneer of authenticity, but with content aimed to defraud us.

Maintaining a healthy scepticism with all communications is therefore critical – whether over email, telephone, texts, social media, messaging platforms or a combination. This is especially the case when a communication is

unexpected, makes you feel something and asks you to do something. Social engineering uses emotional bait to cloud our judgement before pushing us into an action, such as clicking a link, downloading an attachment, sharing information or transferring money.

If in any doubt, check with the supposed sender via another channel to verify that the person you are communicating with is who they say they are – especially if you are being asked to transfer money, share information or click a link.

Practising positive security behaviours described elsewhere in this book is also vital, including securing our online accounts with multi-factor authentication as well as strong and unique passwords, keeping devices up-to-date and using anti-virus software. Report or flag suspicious emails in your inbox, so that your IT department at work (or email provider) can identify phishing emails as soon as possible and be in the best position to mitigate any potential harm from them. Social media platforms and other online services generally have ways to report phishing content and by doing so you are helping to flag this content and keep other people safe by limiting its spread.

Remember that the right phish at the wrong time can catch any of us. We can all have days where we are busy, distracted, stressed or vulnerable. We all have the potential to be manipulated by experienced, trained, skilled and practised criminals. This does not mean we should be paranoid; it simply means we should exercise caution and be mindful.

Notes

1 FBI IC3 (2023) Federal Bureau of Investigation Internet crime report 2022. www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf (archived at https://perma.cc/6J6N-3HGH)

2 Comcast Business (2023) 2023 Comcast business cyber security threat report. business.comcast.com/community/docs/default-source/default-document-library/ccb_threatreport_071723_v2.pdf?sfvrsn=c220ac01_3 (archived at https://perma.cc/9N34-JR5B)

3 Anti-phishing working group (2022) Unifying the global response to cyber crime. docs.apwg.org/reports/apwg_trends_report_q4_2022.pdf?_gl=1*k3uqak*_ga*MjA4NzMwNjcxMi4xNjk5MTQxMTk2*_ga_55RF0RHXSR*MTY5OTE0MTE5Ni4xLjEuMTY5OTE0MTU3MC4wLjAuMA..&_ga=2.182498086.1619969749.1699141196-2087306712.1699141196 (archived at https://perma.cc/CSF5-433N)

4 Microsoft (2023) What is phishing? www.microsoft.com/en-us/security/business/security-101/what-is-phishing (archived at https://perma.cc/MRY5-LTY2)

5 Verizon (2023) Data breach investigations report. www.verizon.com/business/resources/reports/dbir/ (archived at https://perma.cc/EZ3P-CNFE)

6 Tidy, J (2020) Google blocking 18m coronavirus scam emails every day, BBC News, 17 April. www.bbc.com/news/technology-52319093 (archived at https://perma.cc/R2DP-8URC)

7 Brook, C (2022) Phishing campaigns pick-up in the wake of the Ukraine invasion, Tessian, 5 April. www.tessian.com/blog/phishing-campaigns-pick-up-in-the-wake-of-the-ukraine-invasion/ (archived at https://perma.cc/E3TA-9ZH4)

8 Forsdick, S (2019) How to avoid the email scam that saw Facebook and Google lose over $100m, NS Business, 25 March. www.ns-businesshub.com/technology/email-scam-facebook-google/ (archived at https://perma.cc/QV8F-C249)

9 US Securities and Exchange Commission (2015) Ubiquiti Networks. www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm (archived at https://perma.cc/VPT4-UPSY)

10 Muncaster, P (2018) Save the Children hit by $1m BEC scam, Infosecurity Magazine, 17 December. www.infosecurity-magazine.com/news/save-the-children-hit-by-1m-bec/ (archived at https://perma.cc/PA47-BJQ5)
11 FBI IC3 (2022) Federal Bureau of Investigation Internet crime report 2021. www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (archived at https://perma.cc/M6DT-EETS)
12 FBI (2022) Business email compromise: the $43 billion scam, FBI, 4 May. www.ic3.gov/Media/Y2022/PSA220504 (archived at https://perma.cc/P85H-VPHN)
13 Group-IB (2020) Operation Falcon: Group-IB helps INTERPOL identify Nigerian BEC ring members, Group-IB, 25 November. www.group-ib.com/media-center/press-releases/gib-interpol-bec/ (archived at https://perma.cc/2E5S-6TUL)
14 Renals, P (2020) SilverTerrier: New COVID-19 themed business email compromise schemes, Palo Alto Unit 42, 7 May. unit42.paloaltonetworks.com/silverterrier-covid-19-themed-business-email-compromise/ (archived at https://perma.cc/7MJD-KRCP)
15 Kolmar, C, (2023) The 100 largest companies in Nevada for 2023, Zippia, 21 July. www.zippia.com/advice/largest-companies-in-nevada/ (archived at https://perma.cc/JK6C-PPZ3)
16 Westgate Resorts (2023) 17 fun facts about Las Vegas that will make you think, Westgate Resorts, 4 April. www.westgateresorts.com/blog/las-vegas-facts/# (archived at https://perma.cc/HTT9-K7PV)
17 Smith, C (2023) Annual Disney Park attendance statistics and charts, Disney News, 10 November. disneynews.us/disney-parks-attendance/ (archived at https://perma.cc/W4LJ-YPDX)
18 Stutz, H (2023) MGM's losses in cyber attack will be insured up to $200 million, The Nevada Independent, 19 September. thenevadaindependent.com/article/mgms-losses-in-cyber attack-will-be-insured-up-to-200-million (archived at https://perma.cc/LBQ5-6BEJ)
19 Grantham-Philips, W (2023) Data breach at MGM Resorts expected to cost casino giant $100 million, AP, 6 October. apnews.com/article/mgm-cyber attack-las-vegas-100-million-clorox-087726961b5366065b6231d1d223b4eb (archived at https://perma.cc/RP4Y-E5PW)

20 US Securities and Exchange Commission (2023) MGM Resorts International. www.sec.gov/ix?doc=/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm (archived at https://perma.cc/YD83-WM6R)
21 Target, E (2023) MGM Resorts' ransomware attack started with a single phone call, The Stack, 13 September. www.thestack.technology/mgm-ransomware-attack-social-engineering-linkedin-call/ (archived at https://perma.cc/4F63-PXXP)
22 Morrison, S (2023) The chaotic and cinematic MGM casino hack, explained, Vox, 6 October. www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware (archived at https://perma.cc/E9DV-7ETP)
23 Srivastava, M (2023) MGM hack followed failed bid to rig slot machines, Financial Times, 14 September. www.ft.com/content/a25d2897-b0ce-4ba7-92ed-ff5df09d1b47 (archived at https://perma.cc/4J3P-5U9P)
24 Stone, B (2022) Voice phishing attacks reach all-time high, TechRepublic, 24 May. www.techrepublic.com/article/voice-phishing-attacks-reach-all-time-high/ (archived at https://perma.cc/PH4C-BQX8)
25 Foran, P (2023) TD Bank customer loses $12K to elaborate vishing scam, CV News Toronto, 13 June. toronto.ctvnews.ca/mobile/i-m-terrified-td-bank-customer-loses-12k-to-elaborate-vishing-scam-1.6439843 (archived at https://perma.cc/23HV-FEFU)
26 Summers, C (2023) iSpoof promotional video. youtu.be/y4f0hN4K62g (archived at https://perma.cc/SE3N-6FMF)
27 Eurojust (2023) Main administrator of iSpoof website sentenced to 13 years. www.eurojust.europa.eu/news/main-administrator-ispoof-website-sentenced-13-years (archived at https://perma.cc/3M6W-D6SV)
28 Binns, D (2023) Tejay Fletcher jailed for running multimillion-pound criminals website iSpoof, Sky News, 19 May. news.sky.com/story/tejay-fletcher-jailed-for-running-multimillion-pound-criminal-website-ispoof-12883414 (archived at https://perma.cc/GU4V-8Y9P)
29 PA Media (2023) Fraudster jailed for running multimillion-pound website iSpoof, The Guardian, 19 May. www.theguardian.com/uk-news/2023/may/19/fraudster-tejay-fletcher-jailed-for-multimillion-pound-website-ispoof (archived at https://perma.cc/EMU8-CEAB)

30 Cluley, G (2022) Operation Elaborate – UK police text 70,000 suspected victims of iSpoof bank fraudsters, Tripwire, 24 November. www.tripwire.com/state-of-security/operation-elaborate-uk-police-text-70000-suspected-victims-ispoof-bank-fraudsters (archived at https://perma.cc/77Q9-GHV4)
31 Martin, A (2022) OMG not only have they taken down iSpoof's homepage, but this is what @metpoliceuk uploaded to the service' Telegram channel, 24 November. x.com/AlexMartin/status/1595704261312413696?s=20 (archived at https://perma.cc/K7SW-9MXL)
32 Binns, D (2023) Tejay Fletcher jailed for running multimillion-pound criminals website iSpoof, Sky News, 19 May. news.sky.com/story/tejay-fletcher-jailed-for-running-multimillion-pound-criminal-website-ispoof-12883414 (archived at https://perma.cc/N5UF-P9W8)
33 Robokiller (2022) Car warranty robocalls plummeted in late 2022: here's why, Robokiller, 16 November. www.robokiller.com/blog/2022-car-warranty-call-trends (archived at https://perma.cc/LFX7-NNTS)
34 FCC (2023) FCC orders blocking of calls from gateway facilitator of illegal robocalls from overseas. docs.fcc.gov/public/attachments/DOC-393325A1.txt
35 TransNexus (2023) STRI/SHAKEN statistics from February 2023, TransNexus, 1 March. transnexus.com/blog/2023/shaken-statistics-february/ (archived at https://perma.cc/79VW-LLF7)
36 Proofpoint (2023) 2023 State of the phish. www.proofpoint.com/us/resources/threat-reports/state-of-phish
37 Kalinoski, D (2023) The rise of smishing, AARP, 11 October. states.aarp.org/pennsylvania/the-rise-of-smishing (archived at https://perma.cc/XX66-X7EX)
38 Lakshmanan, R (2023) Spanish police takes down massive cyber crime ring, 40 arrested, The Hacker News, 11 May. thehackernews.com/2023/05/spanish-police-takes-down-massive.html (archived at https://perma.cc/227X-BX2W)
39 FBI (2022) Cyber criminals tampering with QR codes to steal victim funds. www.ic3.gov/Media/Y2022/PSA220118 (archived at https://perma.cc/K49U-8DT9)

40 Sharma, A (2023) QR codes used in fake parking tickets, surveys to seal your money, Bleeping Computer, 8 May. www.bleepingcomputer.com/news/security/qr-codes-used-in-fake-parking-tickets-surveys-to-steal-your-money/ (archived at https://perma.cc/52HJ-QL7E)
41 Lyons Hardcastle, J (2023) Spanish phisherfolk caught in cops' net in multi-million euro catch, The Register, 25 October. www.theregister.com/2023/10/25/spanish_phishing_arrests/ (archived at https://perma.cc/3Z44-7GC5)

CHAPTER TWO

Account compromise

A compromised account can cause many problems, ranging from tedious to deeply troubling. Our online accounts are the key to so much of our information, they are how we connect and communicate with others, and they can be crucial to our professional lives – the organizations we run or work for.

This was the case with Nikki Golding and her children's clothing firm, Rose and Guy. For eight years, Golding built her small business and by the summer of 2023 her business Instagram page had nearly 50,000 followers with 95 per cent of her business generated via the social media site. Within three days of losing her hacked account, Golding was receiving zero orders.

As her mobile phone number was linked to her Instagram account, the criminals were able to contact Golding. They sent her WhatsApp messages for days following the compromise, attempting to extort £300 from her for the return of the account and threatening to sell her account if she did not comply. Golding refused to pay:

> 'I didn't want them to think it was acceptable to continue to do it to others. I thought, if I pay then they've won.'[1]

Golding had two-factor authentication on her account, so the criminals could not change the email address linked to it. That meant she was able to remove them from the account and report the compromise to Instagram, preventing the criminals from using her account for further malicious purposes, such as trying to phish her followers or spread scams and disinformation. However, she still could not get her account back. After about a week of trying to get Instagram to return her account, she accepted that she would not get the account returned to her:

> 'All I kept thinking about was what happened. I was so upset, angry with the hackers and felt let down by Instagram. I just burst into tears… People need to see just how awful this is and how much it can affect someone's life. I know it's only Instagram but that is my business, and it is my life.'[2]

She created a new Instagram page, starting again with zero followers, and shared a video about her experience on a new TikTok account. The video showed Golding in tears, with a description of how hard she had worked, showing screenshots of the criminals attempting to extort her. The video went viral, with celebrities and influencers sharing it,

and within three days her new account had reached nearly 70,000 followers. Rose and Guy went on to receive more orders than ever before.

Golding's story had a happy ending. She experienced distress as a result of the attack, and her business had a temporary hit which could have been devastating, but her positive use of technology ultimately overpowered the criminal's abuse. Unfortunately, not all account compromise works out so well for victims, and keeping our accounts safe is vital for protecting our information, our communications and our finances. So, how do criminals compromise our accounts? Let's dig into passwords, two-factor authentication and more.

Passwords

The first computers were huge, expensive machines, and most were purpose-built. Digital security was not really a consideration at the time. By the late 1950s, computers had become usable to the extent that universities were now utilizing them for projects. It was a very different picture to the way computers are used in universities today. A single disk could only hold around 5MB of data so computers were shared: everyone kept their files together and with no passwords, people could accidentally (or intentionally) access everyone else's work, or, worse, delete it.

It was the summer of 1961 when Fernando Corbató created the first password system. He was working at the Massachusetts Institute of Technology (MIT) and, in a bid

to wrangle the computer users, designed a project to fairly share the time available to projects. With time limits for projects set to just four hours a week, it wasn't long before people started to steal each other's passwords: Allan Scherr, an MIT researcher at the time, is the first known password thief, which he has embraced as 'really something to be famous for'.[3]

After the chequered success of that project, passwords took off, although security was not always the goal. In a 2004 interview with a former Minuteman Missile officer, Dr Bruce G Blair revealed to the world that the 1970s defence system was protected from launch by an eight-digit passcode, which was '00000000'. Not only was that the code for the silo that Blair oversaw, but for all the missile sites across the US – and not only was this incredibly weak passcode used universally, but it was also not even a secret. In every manual on the launch procedures, the passcode was printed clearly. Anyone that had access – including civilian contractors – could see it. The commanders worried more about the time-to-launch rather than unauthorized launching; concerned that if communications with the President failed at a crucial time, they would still need the ability to launch a counter-offensive.[4]

Their fears were not misplaced: similar authentication codes carried by presidents have been lost before. President Carter lost his due to a dry-cleaning incident and President Reagan's were taken by accident by the FBI when they took his clothes during his recovery from an assassination attempt in 1981.[5]

So, although passwords are a technical layer of defence on our internet accounts, there is a very human element to the codes.

How passwords are compromised

Passwords can be compromised in multiple ways: they can be stolen via malware (see Chapter 9), we can be manipulated into sharing them (as we explored in Chapter 1) and they can be guessed or cracked.

To understand how passwords are cracked, we need to start by taking a step back. Let's say you use a password of '23BrightBlueBananas!' for one of your online accounts. The site stores it securely by applying mathematics, via an encryption algorithm which turns your password into a long string of numbers called a hash. When you enter your password to log in to the site, the system performs its mathematical magic, generating the string of characters and comparing them to the one that it stored when you created your account: if the strings match, then you are let into the account. If a criminal gets their hands on the encrypted hash, for example by breaching the website, they theoretically should not be able to reverse engineer your password from the hash if that is all they have, even if they know what algorithm was used to create it (of course, different algorithms have different performance and weaknesses).

However, there are several methods that can enable attackers to gain access to our accounts by compromising the passwords. If an attacker has breached a website and has a database of encrypted passwords (or if they have purchased it from other criminals on the dark web), the simplest way of trying to decrypt the passwords is to merely 'guess' them. They use computer programs to do this, which try to match millions of potential passwords

every second to the encrypted strings. The first thing they are likely to try are known words, known as a dictionary attack, mostly because they throw the entire dictionary at it. Even if your password is 'pneumonoultramicroscopic-silicovolcanoconiosis' – the longest word in the English dictionary – if attackers try every word in the dictionary, they will eventually 'guess' it. Most savvy attackers know that people commonly use hobbies, sports teams and fandoms as passwords, so they include those in dictionary attacks, too. Password such as 'LiverpoolFC', 'Eminem' and 'Starwars' are all easily compromised in a dictionary attack.

The attacker will add permutations to improve their chances of 'guessing' the password. As well as trying all dictionary words and known phrases, they will script the program to account for the little tricks we use, for example adding a 1 or ! to the end or adding dates, for example 'England1966!'. These rules and permutations make it easy for the attacker and harder for us to come up with secure passwords to stop them.

Most passwords that people currently rely on would not survive a dictionary attack. In the scenario above, a criminal is likely to come away with approximately 80 per cent of the passwords, which they would then use to access the accounts associated with them (as long as multi-factor authentication does not keep them out, as we will see later in this chapter). Many criminals will then give up on the remaining 20 per cent. However, if the attacker has a specific target in their sights, and that password has survived the dictionary attack, they could move on to the slower (but far more certain) method of brute force.

To understand brute force, we will take a little holiday. Imagine you fly abroad to sunnier climes, and you lock your suitcase with a four-digit code. But when you arrive at your destination, eager to don your swimsuit and flip-flops, you can't remember the code! Your first step is essentially a dictionary attack: you try to guess the code by using obvious ones, such as 1234 and 2024. If that does not work, you turn to a brute force attack, trying every number combination you could possibly have on a four-digit lock. From 0000, all the way to 9999, you are guaranteed to find the code. The same method can be used to crack passwords. Try every combination of upper- and lower-case letters, plus numbers, and you will crack any password that uses a combination of those. If we take a random password such as 'A7dh2U', for example, it will eventually be cracked. The good news is the longer and more random the password, the longer it takes to crack (as long as the password is long, complex and not based on known words or phrases). Our example password of just 6 characters is comprised of a combination of 26 lower-case letters, 26 uppercase letters and 10 numbers. This means there will be 58,800,235,584 possible passwords to try. Add another letter to make our password seven characters long and the possible combinations go up to 3,521,614,606,208. The speed at which computers can perform this brute force approach is determined by the speed of the computer and the type of algorithm used.

The above is why classic cyber security advice is to use long, complex passwords that are not based on dictionary words. The other piece of classic password advice is to use unique passwords and not to reuse the same passwords

over different accounts. If a website where you have an account is hacked, the attackers are likely to steal the stored usernames and passwords. Using the methods above, they will attempt to 'guess' or crack the passwords in that database. With the stolen usernames and cracked passwords from the breached data, they will then perform what is known as credential stuffing, taking the usernames and passwords stolen from one site and attempting to use them to access accounts across other websites. Again, this is not something they will do manually, but rather by using automated computer programs.

In December 2022, PayPal discovered that criminals had used credential stuffing to gain access to nearly 35,000 accounts. This meant that the attackers had access to the personal and financial details stored in those accounts. As soon as PayPal realized, they reset the passwords of those compromised accounts and so kicked the criminals out, seemingly within two days of the unauthorized access of accounts.

Passwords alone were never going to be enough to keep our ever-growing online accounts safe. In 1996, AT&T described a method for using two-way pagers to add an extra layer of security to our accounts. This was the start of what we today call two-factor authentication (2FA), using two separate systems to verify our identity. Adding extra layers of security to our online accounts is more important than ever, with stolen credentials being one of the main ways that attackers compromise us at home and at work.

SMS 2FA

Two-factor authentication (2FA, sometimes also referred to as MFA – multi-factor authentication) is a way of adding another layer of security to online accounts, so that they do not just rely on passwords. When we set up 2FA, we must provide two different authentication methods to verify our identity: something we know, such as a password, and something we have, which is most commonly a one-time code which is sent to your mobile phone via text message. Using this method of 2FA is more secure than simply relying on a password to secure your account.

However, this method is vulnerable to an attack known as SIM swapping. In a SIM swap attack, criminals contact your mobile provider and socially engineer them into activating another SIM with your number attached. In this way, they take control of your phone communications by routing your phone to a SIM in their possession and so 2FA codes sent to your phone are now sent to them. In 2022, reports to the FBI reflected victim losses of over $70 million associated with SIM swap attacks.[6]

In December 2021, Nicholas Truglia pleaded guilty in a New York court to conspiracy to commit wire fraud, as part of his role in a group alleged to have stolen more than $100 million from cryptocurrency investors using SIM swapping scams. Truglia admitted that he had been part of a scheme to steal over $20 million worth of cryptocurrency from Michael Terpin, a cryptocurrency investor and co-founder of the first angel investor group for Bitcoin enthusiasts.[7] Truglia had convinced an AT&T employee to transfer Terpin's phone number onto a new SIM, which

meant that he and his associates could breach Terpin's accounts, accessing his email and cryptocurrency wallet passwords. With this information, they stole Terpin's funds and moved the currency into Truglia's own cryptocurrency wallet.

Court documents suggest that Truglia lived a life of luxury from the proceeds of his crimes, with expensive watches, a $6,000 a month apartment and $100,000 in cash kept on hand. In a Twitter account which supposedly belonged to him, he bragged of SIM swapping his father and lamented, 'stole 24 million but still can't keep a friend'.[8] The documents also suggest he boasted to friends, 'Nobody can put me in jail. I would bet my life on it, actually'.[9] In December 2022, Truglia was sentenced to 18 months in prison for the SIM swap attack and theft of Terpin's cryptocurrency; he was also ordered to return the stolen funds to the victim within 60 days. In January 2023, Truglia was released from jail and went to live with his father in Florida. Four months after his release, he was arrested again for alleged fraudulent activities alongside carrying a concealed weapon.

Stronger 2FA

In 2021 and 2022, SIM swapping made headline news around the world when it was used (along with phishing) in a series of high-profile attacks on huge tech companies including Microsoft, Uber, T-Mobile and Samsung. A loose collective, Lapsus$, began their attacks by obtaining basic information about their targets, such as names and phone

numbers. They then used various techniques (including purchasing stolen credentials and using voice, phone and SMS phishing) to take over accounts of employees at telecom providers and used this access to perform SIM swap attacks. The group also recruited malicious insiders at target organizations, advertising offers of up to $20,000 per week for insiders at telecom providers who could conduct SIM swaps.[10]

Once they had completed the SIM swap attacks, they used credentials they had stolen or phished at the target company – along with 2FA codes that they were now receiving thanks to the SIM swapping – to take over online accounts at their targets. From there they used malware and tools to steal further credentials, stole data from their victims, deleted data, stole cryptocurrency and infected victims with ransomware, attempting to extort them. In March 2022, a 16-year-old from Oxford was arrested, alleged to be one of the leaders of Lapsus$ with a $14m fortune amassed from his activities; in total, City of London Police have arrested seven teenagers in connection with Lapsus$[11] and another suspect was arrested in Brazil.[12]

To avoid the dangers of SIM swap associated with SMS 2FA, we can use stronger mechanisms as our second token. Rather than having a SMS code alongside our password, we can use authentication apps,* hardware authentication† or biometrics.

---

*Authentication apps are mobile or desktop applications that generate one-time codes.

†Hardware authentication uses physical devices, such as security keys or tokens.

2FA fatigue

As part of their social engineering methods, Lapsus$ took advantage of 2FA fatigue with 2FA bombing. This attack takes different forms, but often includes the criminals sending multiple 2FA requests to the target, overwhelming them with notifications until they authenticate a login request simply to make it stop. Even though they did not prompt the 2FA request, being inundated with relentless requests pushes the target into unknowingly or unwillingly click to approve the 2FA request, especially if the attackers get the timing of their 2FA bombing right.

In the Telegram channel that Lapsus$ used to communicate, a member of the gang wrote 'no limit is placed on the amount of [2FA] calls that can be made. Call the employee 100 times at 1 am while he is trying to sleep, and he will be more likely to accept it'.[13] They claimed that the technique worked in an attack against Microsoft earlier that week.

To combat 2FA fatigue, service providers are building in mechanisms to tighten the authentication process. For example, Microsoft has implemented a system of number matching which increases the difficulty of quickly or inadvertently approving 2FA requests, adding a manual process to help the recipient be more aware of 2FA requests that they did not prompt.

Password managers

While we have been making advances in the extra layers of security we add to online accounts, the number of the

online accounts that we all have has continued to grow. Couple this with a rise in data breaches exposing our credentials, and it is clear that we cannot generate and remember unique, complex, non-dictionary passwords in our brains:

> 'Asking users to recall a single password and user ID for one system may seem reasonable, but with the proliferation of passwords, users are increasingly unable to cope…
>
> … recalling strong passwords is a humanly impossible task because strong passwords are non-meaningful items and hence inherently difficult to remember.'[14]

Enter: the password manager, a tool to help people generate, store and use passwords across multiple accounts. Rather than having to think of random, unique passwords for every account, a password manager can create them in the click of a button, meanwhile saving them all in a vault behind one master password. In 2002, the first password manager was created by Bruce Schneier. Called Password Safe, Schneier created it as a free utility to help people with a simple, single solution to keeping passwords safe. There is now a whole industry around password managers, with many different solutions on the market.

The number one question with a password manager is: what happens if the password manager is hacked?

From August to December 2022, LastPass suffered two major (connected) incidents. The first attack compromised a software developer and internal confidential company data was stolen. Unfortunately, part of that data was used to launch the second attack against a more senior member of LastPass, who had access to backups of customer

password vaults. This meant that attackers stole all password vaults belonging to LastPass customers. These vaults were encrypted and only able to be decrypted using the customer's master password (which LastPass do not store).[15] If the criminals were able to guess the master password, they would have access to all data saved by a customer in their vault. Several months after the LastPass attacks, researchers discovered that all 25 victims of a $4.4 million cryptocurrency theft stored their crypto-wallet credentials in LastPass.[16] The LastPass case highlights the importance of having strong, random and unique passwords – especially for the master password of a password manager. It is also a reminder to change passwords if there are indications that those passwords may have been compromised.

The number of breaches associated with password managers is very low and the fall-out from them is much less than the impact of breaches and attacks that exploit weak or re-used passwords. The companies running password managers make their living protecting our data, so they are financially invested in being as secure as possible. However, not all password managers are equal, and it is important to choose a reputable and trusted password manager.

Advice for securing your accounts

There are steps we can all take to reduce the likelihood of our accounts being compromised. This starts with being aware of the value of our accounts and how criminals seek to take them over.

Passwords are the major keys to your accounts – and as such they are highly attractive to cyber criminals. To enable your passwords to fulfil their role as the underpinning of your account security, it is important to use long, complex passwords that are not based on known words and phrases. Using unique passwords (rather than reusing a password across more than one account) prevents credential stuffing attacks, as we covered in this chapter.

The need to use complex, random and unique passwords for our growing list of online accounts creates a cognitive load that is impossible to manage if you are attempting to use your brain alone. Therefore it is important to have a system to generate and manage secure passwords outside of your head. Storing passwords in your emails, computer spreadsheets or notefiles is not secure – if you are hacked, criminals will very quickly discover and exploit those passwords, making the breach ten times worse. Consider a password manager to do the heavy lifting for you. Use one that is trusted and reputable, making sure that you have a very long, complex and random password for the master password.

Traditional cyber security advice was that passwords should never be written down. Most cyber security professionals – myself included – now disagree with this blanket statement. If you are managing passwords at home and you trust everyone you share that home with, then writing your passwords down and keeping them together in one safe place is more secure than reusing weak passwords that you have memorized. Unless you're in a workplace,

writing passwords down is usually better than trying to manage them in your head, because when you do that, you are probably coming up with weak passwords and reusing them. It's more likely that a cyber criminal will crack weak passwords that you're managing in your head than that a criminal will break into your house and steal your written password list. If your password diary is stolen in an unfortunate home break-in, you will know about it and be able to change your passwords. This advice does not apply in the workplace, where many more people often have physical access and writing passwords down would likely be in breach of organizational cyber security rules!

Beyond passwords, it is vital to enable 2FA wherever possible to add an extra layer of security and take the burden off passwords. SMS 2FA is better than no 2FA. However, using other methods of 2FA, such as authentication apps or hardware tokens, removes the chance of growing SIM swap attacks enabling criminals to compromise your accounts.

Finally, being alert to social engineering is critical to keeping your accounts safe. Many phishing attacks are aimed at deceiving us into sharing our usernames, passwords and 2FA information as a way of getting into our online accounts.

Notes

1 Cyber crime Magazine (2023) Cyber crime radio – Instagram hacked. Didn't pay the ransom, August. soundcloud.com/cybercrimemagazine/instagram-account-hacked-nikki-golding-founder-rose-and-guy (archived at https://perma.cc/MY29-UP56)

2 Ibid
3 Yadron, D (2014) Man behind the first computer password: it's become a nightmare, The Wall Street Journal, 21 May. www.wsj.com/articles/BL-DGB-35227 (archived at https://perma.cc/7WXN-6E6Y)
4 Blair, B G (2004) Keeping presidents in the nuclear dark, Center for Defense Information, 11 February. web.archive.org/web/20040404013440/http://www.cdi.org/blair/permissive-action-links.cfm (archived at https://perma.cc/ZRY5-LD32)
5 McDuffee, A (2017) Jimmy Carter once sent launch codes to the cleaner, and other scary tales of the 'nuclear football', Medium, 21 November. timeline.com/jimmy-carter-once-sent-launch-codes-to-the-cleaner-and-other-scary-tales-of-the-nuclear-football-add77568346e (archived at https://perma.cc/XM74-XJQ7)
6 FBI IC3 (2022) Federal Bureau of Investigation Internet crime report 2021. www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (archived at https://perma.cc/H39P-CU4R)
7 Krebs, B (2021) NY Man pleads guilty in $20 million SIM swap theft, Krebs On Security, 16 December. krebsonsecurity.com/2021/12/ny-man-pleads-guilty-in-20-million-sim-swap-theft/ (archived at https://perma.cc/J3BB-8VT6)
8 Morse, J (2019) The sad story of an alleged SIM swapper who boosted millions, Mashable, 16 January. mashable.com/article/sim-swap-cryptocurrency-theft-nicholas-truglia (archived at https://perma.cc/TKR7-YLQ7)
9 Ibid
10 CISA Cyber Safety Review Board (2023) Review of the attacks associated with Lapsus$ and related threat groups, 24 July. www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf (archived at https://perma.cc/2C5M-THK2)
11 Tidy, J (2022) Lapsus$: Oxford teen accused of being multi-millionaire cyber criminal, BBC News, 24 March. www.bbc.com/news/technology-60864283 (archived at https://perma.cc/4WEG-5PZJ)
12 Arntz, P (2022) Suspected LAPSUS$ group member arrested in Brazil, Malwarebytes, 20 October. www.malwarebytes.com/blog/news/2022/10/suspected-lapsus-group-member-arrested-in-brazil (archived at https://perma.cc/5UAU-JK3H)

13 Goodin, D (2022) Lapsus$ and SolarWinds hackers both use the same old trick to bypass MFA, Ars Technica, 29 March. arstechnica.com/information-technology/2022/03/lapsus-and-solar-winds-hackers-both-use-the-same-old-trick-to-bypass-mfa/ (archived at https://perma.cc/27NA-WHHG)
14 Sasse, M A et al (2001) Transforming the 'weakest link': a human-computer interaction approach for usable and effective security, BT Technology Journal, 19, 122–31, July. discovery.ucl.ac.uk/id/eprint/144215/1/BTTJSECv5.pdf (archived at https://perma.cc/5JWS-JQTY)
15 Toubba, K (2023) Security incident update and recommended actions, LastPass, 1 March. blog.lastpass.com/2023/03/security-incident-update-recommended-actions/ (archived at https://perma.cc/6XNR-RF83)
16 Abrams, L (2023) LastPass breach linked to theft of $4.4 million in crypto, Bleeping Computer, 30 October. www.bleepingcomputer.com/news/security/lastpass-breach-linked-to-theft-of-44-million-in-crypto/ (archived at https://perma.cc/VK8Q-37Z6)

CHAPTER THREE

Vulnerabilities and exploits

When we create something, we often make mistakes. Sometimes, those mistakes are so huge that it becomes immediately obvious we must start again and sometimes, we fix errors as we go. Mistakes can be so minor that they will never be noticed by anyone else and sometimes, we don't even realize the mistakes are there until someone else finds them for us. Other mistakes fit in the 'so what?' category where, although there is an error, it does not actually do any harm. All of this applies to software development, especially with a 'move fast and break things' culture in many companies that pushes software developers to be as productive as possible so the company can be the first to market. Errors in software development can cause security vulnerabilities (also referred to as bugs).

To take advantage of a vulnerability, attackers need to create an exploit – while a vulnerability is the root cause of the issue, it is exploits which really do the harm. There are many security vulnerabilities (known and unknown) in software, systems and devices, but criminals need to develop, buy or otherwise use exploits to be able to abuse that bug and get into networks, steal data, steal information, or otherwise damage the organization. In 2022, the three main ways that attackers gained unauthorized access to organizations were via stolen credentials (as we covered in Chapter 2), phishing (Chapter 1) and exploitation of vulnerabilities.[1]

In May 2023, the Russian ransomware gang Cl0P gained access to MOVEit, a piece of software designed for the safe transfer of data for companies that need to securely move sensitive files. The criminal group used their access to place a backdoor in the software, meaning they could gain further access into the companies using the MOVEit software – and that was a lot of companies.

Within a few days, the evidence of damage started to pour in. By mid-June, it was reported that 347 organizations were affected including British Airways, the BBC, multiple US federal agencies, 58 US educational institutions, energy companies and banks.[2] Cl0P stole sensitive data, sharing the names of victim organizations and threatening to leak the data if a ransom was not paid.

The US government contracting firm Maximus confirmed that the personal information (including health data) of up to 11 million individuals was accessed from their systems as a result of the MOVEit breach, with a class action lawsuit subsequently launched against them.

Unfortunately, the number of affected companies keeps climbing as we continue to hear about new cases. By November 2023, analysis suggests that over 2,500 organizations have been breached, affecting over 67 million individuals; over three-quarters of the victim organizations are based in the US and education is the most heavily impacted sector (41.3 per cent), followed by health (19.2 per cent).[3]

Progress, the company which owns MOVEit, acted quickly in response to the identification of the vulnerability. The criminal infiltration was identified on 28 May 2023 and by 31 May, Progress had already issued a patch to the flaw that the criminals were exploiting. This meant that companies using MOVEit could, in theory, simply apply the patch and stop attackers from using the flaw as a way into their networks. However, as I will explore in this chapter, cyber security is rarely so simple.

The MOVEit compromise tells us a lot about the cyber security challenges of supply chain attacks: when a company that lots of other organizations rely on is compromised, it can deeply affect all of those in the chain, as well as their employees, customers and their suppliers. MOVEit also shows us the impact of exploited zero-day vulnerabilities.

Zero-day vulnerabilities

The MOVEit attack exploited a zero-day (also known as a 0-day) vulnerability, meaning a software vulnerability or security flaw that is unknown to the software vendor and the public. As a zero-day vulnerability is not yet discovered

or disclosed, the software vendor has 'zero days' to address and fix the issue.

Zero-day vulnerabilities are highly sought after by cyber criminals and hackers because they can be exploited before the software vendor has any awareness of the issue; before they have a chance to release an update (also known as a patch) to fix the vulnerability. By definition, we don't know about zero-days, so we aren't even looking for them, let alone fixing them. This makes them doubly dangerous.

The summer of 2023 has been referred to as the 'hot zero-day summer', with 70 previously unknown vulnerabilities discovered by September.[4] With these numbers, it looks like 2023 will set the record for the most zero-days in a year. When zero-days become known to the vendor, they can work on a patch to protect people who use the software or device. In September of 2023, you probably had to update the software and devices you were using more than once; with 12 zero-days discovered in the wild in that month alone, Apple, Microsoft, Google and many other large technology vendors had to release updates.[5]

Zero-day vulnerabilities often have a big impact on cyber security. They also capture the headlines. However, most vulnerabilities discovered in corporate networks are not zero-days. Researchers at F-Secure found that 61 percent of vulnerabilities discovered in corporate networks in 2021 were at least five years old[6] and the cyber security company Securin found that 76 per cent of vulnerabilities exploited by ransomware in 2022 were discovered between 2010 and 2019.[7]

N-day vulnerabilities

In the winter of 2022 to 2023, US authorities identified that a federal agency had been compromised by multiple attackers, one working on behalf of another nation, believing that one group had begun exploitation in August 2021 and another in August 2022. The attackers had exploited a known vulnerability with a severity rating of 9.8 out of 10 and which, in 2020, the National Security Agency (NSA) had warned was being exploited by Chinese state-sponsored attackers.[8]

When a vulnerability is discovered and disclosed – becoming public – it is no longer a zero-day and becomes an N-day (or 1-day) vulnerability, a known security flaw for which a patch either is or is not available. The 'N' in 'N-day' represents the number of days that have passed since the vulnerability became publicly known or was discovered. Attackers use automated software and tools to scan networks and systems searching for N-days with an aim to exploit them.

In 2017, the credit reporting company Equifax reported a data breach that had exposed the personal information of 145 million Americans (approximately 40 per cent of the population at the time), including Social Security numbers, passports and driver's licenses. More than 200,000 records also included credit card numbers. Attackers took advantage of a vulnerability that had been discovered and issued with a patch just weeks before. The attackers discovered a customer complaint website used by Equifax that did not have the patch applied to it and gained access to the Equifax systems. They were able to

move across their network and find plaintext passwords stored in spreadsheets and note files, before moving into other systems and ultimately remaining in the Equifax systems for 76 days before being discovered.

With the huge amount of personal information that was stolen, many expected a similarly huge rush of identity fraud (see Chapter 6), yet not a single case of ID fraud has been attributed to it. We have seen other high-profile thefts of personal data where, again, no cases of ID theft were attributed, for example the 2014 and 2015 US Office of Personnel Management (OPM) breaches, when 26 million US federal government employees and contractors had their personal and financial information stolen (including 5.6 million fingerprint records).[9]

It seems incredible that this information would not be tied to any cases of identity fraud – until we see the bigger picture of these attacks. In February 2020, the US announced charges against four Chinese citizens accused of carrying out the Equifax breach in a military-backed operation, with US Attorney General William P Barr stating in a press conference:

> 'For years, we have witnessed China's voracious appetite for the personal data of Americans, including the theft of personnel records from the US Office of Personnel Management, the intrusion into Marriott hotels, and Anthem health insurance company, and now the wholesale theft of credit and other information from Equifax. This data has economic value… as well as the creation of intelligence targeting packages.'[10]

Creating a huge data lake of cross compiled information about US citizens would enable state-sponsored attackers

to target specific individuals, specifically finding those in positions of power and in companies of interest. This information would be coveted for many reasons. Cross-referencing it with data from Equifax, it would be easy, for example, to find people in difficult economic circumstances who could be approached as insiders for either commercial espionage or government spying.

The charges announced by US Attorney General William P Barr in February 2020 were not the only crimes associated with the Equifax breach, with other criminal charges closer to home. In June 2019, the former Chief Information Officer of Equifax was sentenced to federal prison for insider trading related to the breach. Jun Ying 'thought of his own financial gain before the millions of people exposed in this data breach knew they were victims' when he allegedly became aware of the breach and sold his stock options, avoiding a loss of over $117,000 when the news went public, and the stock price fell. Ying was sentenced to four months in prison and ordered to pay a fine of $55,000 on top of the restitution amount of over $117,000.[11]

Ying was not the only Equifax employee who profited from the breach before being caught out. In August 2017, Sudhakar Reddy Bonthu was a software development manager at Equifax who became aware that the company had experienced a breach which had affected the personal information of approximately 100 million Americans and that they would announce this on 6 September 2017. Bonthu used this inside knowledge to profit $75,000 on Equifax stocks, before being caught and sentenced to eight months' home confinement, plus forfeiting the funds and paying a fine of $50,000.[12]

The huge fallout from breaches like Equifax and the prevalence of N-day vulnerabilities in corporate networks begs the question, why do some vulnerabilities remain unpatched?

A vacuum of patches

When patches for N-day vulnerabilities are produced and freely available, it can seem preposterous that the associated security flaws still cause so many issues. However, there are several reasons why known vulnerabilities in systems, devices and networks can remain unpatched – some more logical than others.

Technical issues can be a barrier to patching; for example, large, complex systems in some organizations can be challenging, requiring time to test whether applying a patch will disrupt operations. There can be concerns about compatibility and whether applying updates will have an unexpected impact on existing hardware and software, especially if the organization is running custom-built software or applications where patching can be more complicated and costly. Network segmentation is regarded as a fundamental element of cyber security controls, but when it comes to patching, having a highly segmented network can make it difficult to reach isolated areas with regular updates. For example, a government department could have an air-gapped system, meaning one not connected to the internet, most likely to keep it more secure. Automated software updates would have no way of connecting to the air-gapped system, meaning that running an update would

be expensive and time-consuming. On the other side of things, connectivity can also cause a problem – as Chapter 11 will show, smart devices have often lacked mechanisms to be updated, preventing vulnerabilities from being easily mitigated.

Organizational factors can also be a blocker to a healthy patching program. Small businesses and those with limited resources can struggle with time and personnel constraints getting in the way of running regular updates. There can be a lack of awareness in organizations, or cultural blockers to change, which can prevent an understanding of the need to prioritize cyber security and the management of vulnerabilities, causing a failure to establish and deliver regular patching.

In other cases, there can be known vulnerabilities that do not have associated patches. There can be a number of reasons for this; for example, if a security researcher discloses a vulnerability but the vendor does not release a patch for it. A vendor could be in the process of developing a fix to the flaw, or could be in the process of rolling it out to all customers. In legacy systems, where technology is old, organizations may be using systems and software that are no longer supported by vendors, which can mean that they have discontinued patches, leaving the systems at the mercy of new exploits developed for emerging vulnerabilities. For example, let's take a hospital that runs old, expensive medical equipment on an old operating system, from a vendor that no longer supports the machine. New

software is incompatible with the old machine and so the hospital has two choices: buy a new, very expensive machine or continue using the old one without patches for newly discovered vulnerabilities.

The vulnerability ecosystem

How do criminals get their hands on vulnerabilities and exploits? The classic cyber security answer applies: it's quite complicated, and it depends.

There is a wide and diverse vulnerability and exploit ecosystem, a spectrum that ranges from legitimate at one end to illegal at the other, with shades of grey in the middle. On the legal side of things, bugs are privately reported to the vendor or a legitimate third party by hackers and security researchers as part of responsible vulnerability disclosure processes (for example in bug bounties* or disclosures to computer emergency response teams that handle security incidents at a national level). At the far end of the ecosystem, criminals buy and sell vulnerabilities and exploits on the dark web. Existing in a grey area in the middle are exploit brokers whose legality is determined based on who they trade with.

Attackers often share information with each other in online forums, social media and messaging platforms. In October 2015, the UK telecom company TalkTalk

*A bug bounty is a reward given to ethical hackers and security researchers who discover and report security vulnerabilities, often as part of defined programs run directly by companies or websites, or via bug bounty platforms.

experienced a cyber attack that exploited a N-day vulnerability in their website, which enabled attackers access to a database of 156,959 customers' personal and financial data. News of the attack dominated the headlines, with TalkTalk initially stating that the attack potentially affected all of their 4 million customers and the then-CEO Dido Harding making multiple media appearances and sharing information that was quickly shown to be inaccurate.[13] Within months of the breach, the Metropolitan Police had arrested six people in connection with it: all male, all under 21 years old and all in the UK. A sixteen-year-old boy who was arrested said he had found the vulnerability and posted details of it on a hacker forum, telling police that he had simply been trying to show off to his mates. Another pair of young men were arrested when one of them exploited the vulnerability, hacked into the TalkTalk website, and downloaded as much data as he could, sharing it with a friend who posted it for sale on the dark web, leading to him and his friend being apprehended by police. TalkTalk was issued with a £400,000 ($530,000) monetary penalty by the UK's Information Commissioner's Office, the largest that had ever been issued.[14] TalkTalk estimated that the breach cost them £60 million ($70 million) and 95,000 customers.[15]

As well as freely sharing information about vulnerabilities and exploits with one another, criminals buy and trade vulnerabilities and exploits, often using the dark web. To understand the dark web, we can use an analogy from the physical world. The surface web is like the public physical space that is freely available for us all to roam around, such as a city centre or public park. We don't need special

permission to be there, or to verify our identity to be allowed entry. So, the surface web is those parts of the internet that we can browse freely, such as search engines and news sites. The deep web is like those parts of the physical world where we need to verify that we are legitimately allowed access before we can enter, for example using a key to enter our home (and perhaps a code, much like two-factor authentication, to turn off an alarm) or a keycard to enter our workplace. This is very similar to the deep web, those online accounts such as social media and email, where we need a username and password (plus, hopefully, two-factor authentication verification to enter – as we covered in Chapter 2). Finally, we have the dark web, which is very different. We need a different type of technology to get there; you can't just stumble upon it. It's a bit like going to space: you need a rocket. But, in this case, your rocket is a different type of web browser that can simply be downloaded. While many legitimate platforms and websites are on the dark web, it is also a haven for criminals who exploit the greater anonymity available to run and use Amazon-like dark marketplaces that sell illegal goods and services, including vulnerabilities and exploits, hacking kits and services such as Ransomware-as-a-Service (see Chapter 10).

Zero-days are also sold legitimately. Exploit acquisition platforms work with security researchers and hackers to buy zero-day exploits, which they then sell to institutional clients. Zerodium is one such platform, founded in 2015 in Washington DC, US, who state on their website that they 'take ethics very seriously and… choose our customers very carefully through a very strict due diligence and

vetting process', adding that 'Zerodium customers are government institutions (mainly from Europe and North America) in need of advanced exploits and cyber security capabilities'.[16]

The value of vulnerabilities and exploits ranges from a few hundred dollars to multi-million price tags, depending on rarity and potential impact. In September 2023, Operation Zero offered payments ranging from $200,000 to $20,000,000 for 'top-tier mobile exploits', explaining 'As always, the end user is a non-NATO country' in a post on Twitter.[17] Operation Zero is a company based in Russia, which has 'all required permits to perform business in this field' and state that their clients are 'private and government organizations that are interested in increasing their defensive and offensive information security potential'.[18] The zero-day market has continued to grow over the last two-and-a-half decades, with some research suggesting that the price of certain exploits is increasing by 44 per cent per year.[19]

Vulnerabilities and different devices

Vulnerabilities can affect all devices; for example, vulnerabilities in Internet of Things (smart) devices have been exploited with implications that have been felt around the world (see Chapter 11). And the more that phones and tablets have become computers in our pockets, the more valuable exploits for these devices have become. Research suggests that there are higher prices for exploits which take advantage of vulnerabilities on mobile devices

compared to desktops, and zero-click remote access exploits are the most valued.[20] Zero-click exploits are as the name suggests: they need no interaction from the end user of a device to run.

When Apple released emergency updates on 7 September 2023, they were fixing two security vulnerabilities that researchers at Citizen Lab called BLASTPASS, found to have been actively abused as part of a zero-click exploit chain to deploy spyware onto iPhones. When the malware, Pegasus, infects a device it can spy on SMS messages, emails, photos and videos, contacts, messaging app communications, GPS data, as well as the microphone and camera, and more. Pegasus was created by NSO Group, an Israeli hacking firm that once told Amnesty International that they would do 'whatever is necessary' to ensure their software would only be used to fight crime and terrorism, but whose work has since been linked to a string of regimes using it to abuse human rights and silence dissidents, including the accusation that Pegasus software was linked to the murder of journalist Jamal Khashoggi.[21] Pegasus software is the malware that was reportedly used to spy on Jeff Bezos in 2020, as covered in Chapter 9.

BLASTPASS can be exploited by an exploit chain, meaning multiple exploits are grouped together to compromise a target. Chaining exploits is generally harder and more time-consuming for attackers and can be more difficult to defend against. One of the largest cyber attacks in US history took advantage of four zero-days chained together. In February 2021, approximately 30,000 companies were affected by an attack on Microsoft Exchange servers that handled email for organizations including many small

businesses and local governments. To be able to access the email systems of those organizations, the attackers needed the four zero-day chain of exploits, plus two more conditions to be met: that the organizations be connected to the internet and for them to be running their own copy of Microsoft Exchange. With many organizations still reluctant to trust the cloud, tens of thousands of companies fitted into those categories and were compromised, with attackers believed to be in the emails of those organizations for months before the vulnerability was patched. By July 2021, the FBI attributed the attack to a Chinese-based attack group known as Hafnium.[22]

Managing vulnerabilities and mitigating exploits

There will always be vulnerabilities in code and there will always be those who seek to exploit those vulnerabilities. Our best defence is to fix those vulnerabilities as soon as they become known: if we delay when exploit information is public, then criminals are able to abuse that information and take advantage of unpatched vulnerabilities.

It can feel like security updates always come at the wrong time. How often have you been in the middle of an important email, rushing to meet a deadline or anxious to get on a video call when an update pops up, threatening to slow you down? It can be tempting to delay the update and get on. However, we're always doing something when we're online or using our devices. We don't generally log on for the sake of security. But, if we delay updates, we're playing right into the hands of cyber criminals: when a

patch is released, it's because information about vulnerabilities and exploits is known. When that information is known, you can be guaranteed that attackers of all types are actively trying to abuse the vulnerability and so your device, or data, is at risk.

If you are a business leader or owner, the productivity rate of your organization is no doubt very important to you. But allowing the time needed for a healthy patching programme, and ensuring updates are installed as much and as quickly as possible, can help that productivity so much more in the long-term: there's nothing like a cyber attack to seriously disrupt and delay operations. If you are a software developer or if you lead a team of developers, the first place to start is understanding that there is no code like secure code. As Tanya Janca, founder of We Hack Purple, says:

> 'Software can't be the best without being secure.'[23]

We can think of applying updates as a bit like going to the dentist. There never seems to be a good time, but dealing with issues as they arise is a lot better than trying to deal with an emergency infection.

Notes

1 Verizon (2023) Data breach investigations report. www.verizon.com/business/resources/reports/dbir/ (archived at https://perma.cc/33A2-MJF2)

2 Kovacs, E (2023) MOVEit hack: number of impacted organisations exceeds 340, Security Week, 17 July. www.securityweek.com/moveit-hack-number-of-impacted-organizations-exceeds-340/ (archived at https://perma.cc/J8BR-AL3Z)

3 Simas, Z (2023) Unpacking the MOVEit breach: statistics and analysis, Emsisoft, 18 July. www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/ (archived at https://perma.cc/LYM8-UF7D)
4 Goodin, D (2023) Attack of the 0-days: with 0-days hitting Chrome, iOS, and dozens more this month, is no software safe? Ars Technica, 13 September. arstechnica.com/security/2023/09/with-0-days-hitting-chrome-ios-and-dozens-more-this-month-is-no-software-safe/ (archived at https://perma.cc/L92M-A2UV)
5 Poireault, K (2023) A guide to zero-day vulnerabilities and exploits for the uninitiated, Infosecurity Magazine, 28 September. www.infosecurity-magazine.com/news-features/guide-zero-day-vulnerabilities/ (archived at https://perma.cc/5R5P-RH4H)
6 Pilkey, A (2021) Attack landscape update: Ransomware 2.0, automated recon, and supply chain attacks, F-Secure, 30 March. blog.f-secure.com/attack-landscape-update-h1-2021/ (archived at https://perma.cc/76JL-YZUB)
7 Sandeen, A (2023) The problem of old vulnerabilities – and what to do about it, Dark Reading, 9 May. www.darkreading.com/vulnerabilities-threats/the-problem-of-old-vulnerabilities-and-what-to-do-about-it (archived at https://perma.cc/WZJ7-GH3P)
8 Goodin, D (2023) Pwned: Federal agency hacked by 2 groups thanks to flaw that went unpatched for 4 years, Ars Technica, 16 March. arstechnica.com/information-technology/2023/03/federal-agency-hacked-by-2-groups-thanks-to-flaw-that-went-unpatched-for-4-years/ (archived at https://perma.cc/JX2G-PLT2)
9 Global Resilience Institute (undated) 5.6 million fingerprints stolen in OPM data breach, Northeastern University. globalresilience.northeastern.edu/5-6-million-fingerprints-stolen-opm-data-breach/ (archived at https://perma.cc/3C5D-SRU8)
10 Office of Public Affairs (2020) Attorney General William P Barr announces indictment of four members of China's military for hacking into Equifax, US Department of Justice, 10 February. www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (archived at https://perma.cc/S3ZA-ZDJL)

11 United States Attorney's Office (2019) Former Equifax employee sentenced for insider trading, US Department of Justice, 27 June. www.justice.gov/usao-ndga/pr/former-equifax-employee-sentenced-insider-trading (archived at https://perma.cc/X8ZY-5RZ6)
12 United States Attorney's Office (2018) Former Equifax employee sentenced for insider trading, US Department of Justice, 16 October. www.justice.gov/usao-ndga/pr/former-equifax-manager-sentenced-insider-trading (archived at https://perma.cc/UH4P-HEN7)
13 Barker, J (2015) Talking TalkTalk, cyber.uk, 28 October. cyber.uk/talktalk/ (archived at https://perma.cc/C6UM-WLV5)
14 Information Commissioner's Office (2015) TalkTalk cyber attack – how the ICO's investigation unfolded, ICO. ico.org.uk/about-the-ico/media-centre/talktalk-cyber-attack-how-the-ico-investigation-unfolded/ (archived at https://perma.cc/ZR2K-5G35)
15 Burgess, M. (2016) TalkTalk hack toll: 100k customers and £60m, Wired, 2 February. www.wired.co.uk/article/talktalk-hack-customers-lost (archived at https://perma.cc/ZAG7-GR6U)
16 Zerodium, FAQs. zerodium.com/faq.html (archived at https://perma.cc/2FP8-HNPV)
17 Operation Zero (2023) Due to high demand on the market, we're increasing payouts for top-tier mobile exploits, 26 September. twitter.com/opzero_en/status/1706762507631677760 (archived at https://perma.cc/DT8S-RHB4)
18 Operation Zero, FAQs. opzero.ru/en/faq (archived at https://perma.cc/XGL8-CAEE)
19 Dellago, M et al (2022) Exploit brokers and offensive cyber operations, Cyber Defense Review. cyberdefensereview.army.mil/Portals/6/Documents/2022_summer_cdr/03_Dellage_Simpson_Woods_CDR_V7N3_Summer_2022.pdf (archived at https://perma.cc/8H23-WCGW)
20 Ibid
21 Kirchgaessner, S (2021) How NSO became the company whose software can spy on the world, The Guardian, 23 July. www.theguardian.com/news/2021/jul/23/how-nso-became-the-company-whose-software-can-spy-on-the-world (archived at https://perma.cc/Y4CC-FJLP)

22 United States District Court (2021) Motion to partially unseal search warrant and related documents and [proposed] order, Southern District of Texas. www.justice.gov/media/1136141/dl?inline (archived at https://perma.cc/HC88-F6RW)

23 Haworth, J (2022) 'Security teams often fight against developers taking control' of AppSec: Tanya Janca on the drive to DevSecOps adoption, The Daily Swig, 19 September. portswigger.net/daily-swig/security-teams-often-fight-against-developers-taking-control-of-appsec-tanya-janca-on-the-drive-to-devsecops-adoption (archived at https://perma.cc/WDP6-H5GT)

CHAPTER FOUR

Romance fraud

Romance scams work because we are all human and we can all be manipulated. These scams exploit people who are lonely or looking for love. It's easy to think 'it would never happen to me' or 'I would never fall for that' – and these kinds of comments are regularly left on videos I share about romance fraud on YouTube – but the truth is that many of the scammers who run these operations have a knack for homing in on people at their most vulnerable. These operations are also professional, being run by experienced fraudsters who share their strategies and tactics with one another. When it comes to romance scams, many people fail to appreciate the time and effort that scammers will put into laying the foundation of the scam. Before asking for money, it is most common that these criminals

will ensure their target feels that they are in an established and genuine relationship.

This is why romance fraud is such a big problem. In 2022, nearly 70,000 Americans reported a romance scam, and reported losses hit $1.3 billion.[1] According to these reports, the average loss for each victim was $4,400.[2] Statistics from the UK suggest that the average financial loss for victims in 2022 was £11,796, an increase from £4,720 in 2021.[3] These numbers are only the tip of the iceberg. For a case to be counted in these statistics, the victim needs to be aware that the crime took place (and not still caught up in the scam) and they need to report it to the authorities. Many scam victims do not report the crime to the government, perhaps because they feel a misplaced sense of shame or because they simply do not know who to report the crime to.

Ruth Grover started ScamHaters United in 2014 as a Facebook page, to raise awareness of romance fraud and to support victims. Her husband, having retired from the police force, had passed away and Ruth, a former police dispatcher, had eventually updated her Facebook profile to 'widow'. Very shortly afterwards, she told me – with a smile in her voice – she '*started being very attractive to four-star generals in the US Army!*' – a common cover story for romance scammers. Since then, she and her team of volunteers have supported thousands of victims. The ScamHaters United website – where people can search the name of a new online contact to see if the name has been associated with a scam – has had over 8 million hits, sharing resources to help people understand these crimes as well as crowd-sourcing information on known fraudsters.

The group's Facebook page now has 67,000 followers, with a further 28,000 followers on Instagram and over 34,000 subscribers on YouTube.

When it comes to the scale of romance fraud, Grover states:

> 'This crime is so huge, it is unquantifiable. And yet, still, nobody talks about it.'

The psychological strategy of romance scammers

The criminals running these scams know which emotional buttons to push to lure their targets in and keep them psychologically hooked. One of the main reasons that romance scams are successful is how these operations are run. I say 'operations', because that is what they generally are. We are not usually dealing with individual criminals, but rather well-organized, hierarchical criminal gangs, using playbooks to share their method and detailed techniques with one another.

My first job after completing my undergraduate degree was in a call centre for a supermarket loyalty card. We used a handbook to manage calls with customers. So, if a customer called with a concern that they were missing points, I would turn to page 10 for scripted questions, responses and pointers on how to deal with their concern. If they were moving home and needed to change the address on their account, I would turn to page 6 to run through questions to verify their identity and make sure I had all of the information that my employer needed.

Romance scammers use the same approach. They share a playbook of operating procedures with one another, containing tried-and-tested comments, compliments and questions that they can use to manipulate their targets. When a scammer's target challenges them, for example querying inconsistencies in their story or questioning why they haven't met in person, the scammer can turn to a page of the playbook for a convincing set of lies and evasion to bat the challenge away and keep the target hooked.

This was something which really struck the journalist Hannah Ajala when she was investigating the Janessa Brazil catfishing for her podcast *Love, Janessa*. When I interview Ajala, she commented:

> 'Many of these scammers are so intelligent, they have a frigging handbook. They have conversations with each other in the induction stage and let them know every possible conversation you will have. There is a prompt for that in here. If they're suspicious about why you're asking for money, there's a prompt for that. "You have to remember their birthday to make them feel special". "You have to remember your anniversary, maybe send them a few gifts". And another thing to stress is that it takes a while before any kind of payout is issued.'

Spending weeks, months or even years building their relationship with targets, romance fraud scammers will use techniques such as 'love bombing' to overwhelm their targets with attention and flattery. They will use gaslighting to undermine any challenges their targets have about the legitimacy of the relationship. They may run hot and cold with their target, to keep them hooked. They will wait

until they are confident that their target is hooked, before asking for money. They may elicit sympathy from their victims and convince them that they need money for an emergency, such as medical bills. The scammers are also very controlling, as Grover outlined in our conversation:

> 'Once they get a victim on their chat app, it's "good morning, how was your night?", "how are the weather conditions?", they're texting during the day, then at night it's always "sleep well my angel, I'll see you in your dreams". And so, once they've got their hooks into them, there's always contact and it is a form of control, because they're never letting the victim forget that they're there. As one of my volunteers says, when it was happening to her, she was always waiting for the next dopamine hit. And the scammer is "with" them for 24 hours, for weeks, months, sometimes even years.'

They will often play on the hope of their target, saying that the money is for a flight to finally see them in person. Grover has heard this from victims many times:

> 'I had a lady, who was so desperate to get him [the scammer] home that she'd sent everything she had. Then in one final push, she cashed in her pension pot and sent the money. She never heard from them again. She was physically reeling from what had happened because she could not believe it. It's hard to believe anybody can be this cruel.'

With such a callous crime, it is hard to understand how the criminals perpetrating the scams can sleep at night. It is even more disturbing to know that some of the people behind these scams are being forced into it (see Chapter 7).

But, for others, they find ways to depersonalize their victims, to compartmentalize and justify what they are doing. Having spoken with many romance fraudsters as part of her work, Grover shared:

> 'They can always justify it, but of course there's no justification. And they're so divorced from it, in other parts of the world from their victims mostly. I asked one of them "the man you use in the picture, what do you think about him?" and there was a silence, almost as if "well, nothing". I asked him, "if I showed you different pictures of your victims – or clients, as they like to call them, they don't like the word victim – would you know who they were?" and he said "no, they're just clients". There's no emotion, this is purely money-gathering, they've found a way to do it and they find it easy.'

The geographic distance and online dimension of romance fraud adds weight to the scams. When an online connection is made between two people in different countries, it makes sense that they would usually not have much opportunity to see one another in person. This creates plausible circumstances for fraudsters to build up 'relationships' with their victims without needing to explain why they can't see one another in person. With the Covid-19 pandemic, this accelerated. As Ajala commented:

> 'Obviously in Covid these scams increased, we're all online much more. We were all much more isolated of course. And that online element of it, I think is really interesting in accelerating that closeness because messages can keep just coming in, coming in. And so in a shorter space of time,

> maybe those relationships can feel more embedded and more real than if it was just in the real world.'

Scammers operate using fake identities, taking images and information from unknowing individuals to create a persona for their target to fall in love with. This is called catfishing. With the rise of deepfake technology, it is becoming even easier for criminals to generate false – and convincing – images to use in their fraud (for more on this, see Chapter 13). For many years, while raising awareness of romance fraud and similar social engineering attacks, I would recommend that people run a reverse image search to identify whether the picture of the person they are communicating with belongs to someone else or has been associated with other scams. While that advice is still valid, it is unfortunately becoming less reliable as AI technology allows us all – including criminals – to create completely fake, new images that are not even of real people, and which have no trace on the internet or through a reverse image search.

The US Federal Trade Commission (FTC) tracked the lies that criminals use in romance scams. Analysing over 8 million reports that indicated a financial loss, the FTC found that the most common lie used is 'I or someone close to me is sick, hurt or in jail', with 24 per cent of scams using this hook. Following this, 18 per cent of scams used 'I can teach you how to invest', 'I'm in the military far away' and 'I need help with an important delivery'.[4]

Romance fraudsters will often use convincing pretexts and personas, for example claiming that they are oil rig workers or in the military. This provides a rational cover as to why they cannot meet their target in person, it

accounts for any gaps in communication and, in the case of military personas, it can provide an explanation for any secrecy.

When you are the catfish

Ade Clewlow MBE is a cyber security leader and strategic adviser with a long and decorated military career. I first met Clewlow at a UK government security event and, in writing this book, I asked him to tell me about an experience where he discovered he was – unknowingly – at the heart of a romance scam.

In 2004 and serving in the UK military, Clewlow was deployed to Baghdad and, while serving, kept an online diary with some pieces also published on the BBC website alongside photographs of him. One photograph showed Clewlow in uniform surrounded by camels in the desert at the Kuwait border.

In 2007, back in the UK and at staff college, Clewlow received a 'peculiar letter'. He described receiving the envelope and, before even opening the letter, knowing that there was something odd about it. The envelope was addressed to Major Clewlow – rather than his correct rank of Lieutenant Colonel and sent to the wrong army base, before being forwarded on to his correct location.

Inside the envelope, was 'a very personal letter' in which the writer 'explained that she had been communicating with a British soldier, that over time she had fallen in love with that British soldier and that British soldier was you'. Clewlow had never met or communicated with the woman

and had no knowledge of her or the 'relationship' which had been fabricated without his knowledge:

> 'What struck me and what still sits with me, is that it must have taken tremendous courage for her to write that letter… Once she realized that she had been scammed, once she realized that she had fallen in love with someone who clearly didn't exist, she was then clearly motivated to find out who this person was.'

Before he had a chance to start unravelling what was happening, he was called for a meeting with military intelligence who had discovered that Clewlow had been caught up in a scam. The officer 'used it as a great opportunity to say "Sir, you're all over the internet like a rash and you need to reduce your footprint"'.

The criminals behind romance fraud operations use the internet to run their scams in multiple ways. As in Clewlow's case, they use websites to harvest images of real people to be the unknowing face of their scams. Increasingly, they will use AI to generate these images, but for the time being they have relied on stealing images of real people to manipulate targets into falling in love.

Social media and romance scams

As well as Clewlow, this is also the case with Janessa Brazil, the subject of the BBC podcast *Love, Janessa*. Journalist Hannah Ajala went on a quest to find Janessa in the podcast, and she spoke to me about the search: 'once you search her name, you are inundated with thousands and

thousands of photos'. Janessa was an adult entertainment star, so there were lots of images of her that criminals have used to pose as her and carry out romance fraud. As the podcast chronicles, Janessa appears to be the most impersonated woman in the world.

However, with the rise of social media, many of us (myself included) share pictures of ourselves and our lives. Photos showing us in a work setting, home setting, going out dressed up and at home relaxed. Selfies, photos with family, friends and pets. Photos on holiday, photos of our hobbies, photos of our hometowns. The kind of photos that you – or a scammer – might share with a new online love interest depicting your full life.

In short, social media can be a treasure trove of resources for a scammer to use to catfish unwitting victims.

The FTC also found that it is most common for romance fraud to begin on social media: 40 per cent of people who lost money to romance fraud in 2022 said it began on social media, compared to 19 per cent who said it started on a dating website or app.[5] A theme of romance fraud is that scammers will push their target to communicate over a messaging platform such as WhatsApp, Google Chat or Telegram after making initial contact on social media or a dating platform.[6] These platforms are designed for instant messaging and so scammers can use them to accelerate the relationship. They also offer more anonymity and efficiency.

Grover discussed the rise of social media and messaging platforms in relation to the impact on romance fraud:

> 'Once they started to scam on Instagram, that changed things a lot. On Instagram, they do a "spray and pray". They

> just send out hundreds and hundreds of follow requests and little messages to see who they get back. As soon as they get their victim, it's "I'm sorry honey, I'm not always on here, what's your number and let's go to WhatsApp. What's your email address so we can Google Chat?". They can then centralize all their victims in one place, which makes for greater efficiency.'

The psychology of romance fraud

Romance fraudsters rely on multiple psychological techniques to increase the success of their crimes. Because scammers will bombard the target with love bombing and try to lock them in to the relationship, victims become susceptible to sunk cost fallacy, reluctant to abandon the relationship because they will feel they have invested a great deal of time and attention to it. Confirmation bias also plays its part, with victims interpreting any ambiguous information as confirming their belief that the relationship is real. Scammers take advantage of their targets' empathy, claiming they need help from them, as the FTC statistics highlight. The criminals will also use reciprocity, offering to do their target a favour, for example by teaching them how to invest in cryptocurrency or claiming that they have sent their target an expensive gift.

Reciprocity makes us feel that we are in debt: if someone does us a favour, we feel we owe them and must return that favour. It also causes misdirection. The target may dismiss concerns about trust because the scammer hasn't asked them for anything (yet), in fact they have made it

appear that they have done the opposite. So, the target can think 'they must be legitimate because they are giving me something, not asking anything of me'. When the criminal then moves on to attempting to con the target out of money, they may even make it seem as if it was the target's idea.

Ultimately, these scams work because targets are being manipulated by trained, experienced, professional criminals. With their playbook of tactics, the scammers use flattery, sympathy, attention, and many more manipulative techniques to build up relationships that – to the victims – feel very much like a genuine connection.

Romance fraudsters take their time. They know that if they rush the relationship and ask for money early on, they are less likely to be successful, as Ajala highlights in our conversation:

> 'These scammers, romance fraudsters, they work in a very calculated way and they naturally pursue you. They will say all the right things until they can tell they've got you in. And once they've got that element of trust is when they go into it.'

This aligns with Grover's years of experience battling romance fraud:

> 'They will take as long as it takes. If you are talking to them and you say, "don't ever ask me for money because I've been a scam victim before" they'll make a little note, "don't ask too soon". So, they will talk to them for months more because they are scamming 100 others who are paying. It's not a one-to-one, it's not that they finish with one victim and move to the next. They are getting money all the time so they can be very patient with the ones they need to be patient with.'

Research in the UK found that those aged 51–65 account for almost half of cases of romance fraud where money was lost in 2022. Although there are trends in romance scams, ultimately this crime does not discriminate: there was an 80-year age gap between the youngest and oldest victims of romance scams reported to TSB Bank. In most of these cases, the criminals involved requested money to pay bills and cover the daily cost of living, and in 10 per cent of cases victims sent money to scammers to pay for trips so they could meet in person.[7]

The financial impact of scams and fraud can be devastating for victims. Between 2019 and 2022, almost 30,000 cases of romance fraud were reported to police in the UK, costing £316,878,696 in financial losses.[8] Statistics show that – of reported romance scams – most money lost was transferred via cryptocurrency (34 per cent) and following this was bank wire transfers or payments (27 per cent). However, more people paid the perpetrators of romance scams with gift cards than any other means.[9]

The impact of romance fraud on victims

Romance scams make up a small percentage of fraud overall, with research showing that it accounts for 4 per cent of all (reported) crimes.[10] However, the psychological impact on victims can be deeply cruel. Research has found that victims of identity theft experience emotional and physical symptoms. When the crime is romance fraud, this can be even more profound because the impact can be a 'triple-hit'. Victims experience a financial loss and the loss of a

relationship. They can also find themselves the victim of identity theft, with scammers using the information they glean from their targets to pose as them and commit fraud. For Ruth Grover's work supporting victims, guiding them through this 'triple-hit' needs to be done in stages:

> 'At the end of every scam, there is a lot of emotion. But, what we have to do is damage limitation. The scam is not just for money. From the first "hello", it's "how old are you?" then later "when's your birthday honey?" and then "I'd like to send you a little present" and so it's your name, address and date of birth. They're getting a lot of information for identity theft. And it's put in such a way that victims never think it's happened to them. So, we've got to ground them [victims] before we can let them grieve, because as we're getting them out [of the scam], I don't want them getting whacked with a bank account they didn't know about, or a credit card or – as one woman got – twelve iPhones from Amazon. So, there's a bit of practicality you've got to deal with and then the money, to each person, is relative.'

People can be traumatized as a result of romance scams, even experiencing post-traumatic stress symptoms, describing the loss as like a 'death' and – in some cases – victims report contemplating suicide.[11]

Having worked in cyber security for over a decade, I have heard from victims of romance fraud on multiple occasions. They have always wanted the communications to remain confidential, carrying a sense of shame that they were 'fooled'. Society stigmatizes people in that position and many people internalize a sense that they were

somehow to blame. This feeling can persist even when the scam was spotted or stopped before any money was defrauded from the victim.

In our conversation about romance fraud and her work advocating for victims, Grover told me about the start of her journey discovering romance fraud and fighting for victims:

> 'I always say that I was lucky, because the one [scammer] that I chose to speak to was the worst scammer on earth and he taught me a lot, that it could never have been real… And with my background [working with the police], anytime anybody tells me something, I want proof. I want to know a bit more. I started to do a lot of research in-depth and I was horrified by what I found. Because I put "widowed" on my page, because I had a dead husband, I was a target and that angered me, because you are vulnerable.'

As human beings, we victim-blame as a way to protect ourselves, telling ourselves that a victim is somehow responsible for a crime because we want to convince ourselves that it would never happen to us. It is a very damaging mentality, which causes further harm to a victim, and which lulls the victim-blamer into a false sense of security. As Ajala commented in the wake of her investigation: 'it can happen to anyone'. Grover expanded on this:

> 'I've talked to thousands of victims over the years. One hundred per cent of those victims, within the very first part of our conversation, will say "I am so stupid." And of course, they're not stupid, nobody asks for this to happen to them, they trust, and you can't knock yourself for trusting…

Nobody breaks their own leg. They've had something really bad happen to them, they haven't done it to themselves.

I have a woman who lost £500,000 to "Eric Clapton". Speaking to that woman at great length, I came to understand how it happened. You say it and people react, "How could she do that?" but they haven't listened to "Eric Clapton" talk with them 24/7 and they haven't known how much he wanted to go on this tour, but his management just wouldn't give him the money, how awful he felt because he couldn't do what he wanted to do. She had that all the time, in her head, on her phone, constantly coming to her.

I would like £1 for every time somebody has come to me and said: "I need to tell you, before we talk, I'm educated and intelligent. I never thought it would happen to me". It depends on what day of your life that the scammer makes contact. On some days, you would not fall for it. But, if they got you on a day that something's gone wrong, you're a bit depressed and then you have this nice, smiling, very polite, very sweet, very understanding person wanting to chat to you and you think "you know, that's just what I need". Nobody can judge because you don't know how you would react to it on any given day. I have spoken to victims from every walk of life.'

Sextortion: image-based sexual abuse

In some cases of romance fraud, scammers will convince their victims to share intimate photographs and videos of themselves. This is image-based sexual abuse, otherwise

known as sextortion. The criminals may use explicit images or videos of the person they are catfishing to generate that sense of reciprocity: 'I' have shared these images of 'myself', why won't you do the same in return?

For the target of sextortion, they believe that they are taking a close and intimate relationship to the next level. The scammer has built trust with their victim and used various techniques to make the connection appear real. Victims may even feel that this is the person they will spend the rest of their life with. However, after the victim shares images or videos of themselves, the scammer will threaten to share them publicly or with the victim's family, friends and online contacts. They will often use this threat to blackmail the victim, demanding money, or more explicit images. The FBI received 7,000 reports of online sextortion in 2022 and most of the victims were boys; tragically, more than a dozen victims are reported to have died by suicide in the US alone.[12] It is accepted that, unfortunately, the number of reported cases of image-based sexual abuse is a small percentage of the true number of cases.

Victims of romance fraud and image-based sexual abuse commonly feel ashamed, and in some cases this can be reinforced by the attitude of friends, family and wider society. These awful crimes remind us of the need to root our approach to cyber security in empathy and compassion. The more we victim-blame, the more people attach a sense of shame to becoming a victim. The more people feel ashamed, the less they will engage with what we have to say. The less people engage with our messages, the less they know about cyber security and the more potential there is for them to become a victim in the future.

Spotting romance fraud red flags and staying safe

As this chapter shows, romance scammers are adept at manipulation and deceit. However, as Grover commented, 'with scams, one thing I am grateful for is that they use formats'. There are red flags which we can spot to alert us:

1 Scammers will often ask a lot of questions but avoid providing personal information themselves.
2 When they do share information, you may notice discrepancies in their stories or details.
3 Romance scammers often use love bombing and try to accelerate a romantic connection very quickly, for example claiming that they are in love and using affectionate terms very quickly, such as 'baby' and 'darling' (which also helps them avoid constantly keeping track of which of their victims they are communicating with).
4 They will provide excuses for why they cannot meet in person and will often avoid phone and video calls.
5 They will ask for money or encourage you to offer money, claiming that they are in need or can only meet you in person if you cover the costs in advance.

To protect against being a victim of romance fraud:

1 Be alert to the red flags above and help others be aware of them, too.
2 Share details of the relationship with other, trusted people in your life, such as friends and family, especially if you are being asked for money (an external perspective can provide a 'sense check').

3 Don't include personal data (such as your location) in the username of dating profiles and don't send money or share personal data (such as your date of birth or home address) with online connections.
4 Be very cautious about sending intimate images or videos, even if you feel you can trust the person requesting these; be aware these could be used against you and, if you do decide to share images or videos, crop them to avoid including identifiable features (such as your face or any tattoos).
5 Perform a reverse image search of photographs of online connections using Google; click the camera icon next to the Google search field and follow the directions to search either by uploading a file from your computer or dropping the image into the field. Although AI is making the creation of fake images easier, criminals still currently re-use images of real people which may be found via reverse image search.

Grover makes a key point in how to spot a romance fraud, which is the need to be alert to the stories that they tell:

> 'The way you know that you are in a scam is the story they are telling, the story of their life, their work, the reason they need money, why it needs to be in Bitcoin, why they need your bank account. They will never change that.'

For both Clewlow and Ajala, the advice they share is strikingly similar: trust your gut instincts.

Ajala's experience investigating the widespread impersonation of Janessa Brazil and the ways in which her image was used to defraud victims gave her a deep insight into

the operation of these scams. She spoke of the need to trust your instinct and to 'fact check' online connections:

> 'Always trust your gut instincts, the same way you would naturally remember information about someone if you're unsure. If you're getting to know someone online, ask those questions again. Ask them how many siblings they have and then, sometime later, ask again.'

Clewlow's closing words centred on the victims of romance frauds, the reminder that this can have a profound impact on somebody's life, and the advice for anyone reading this who may be striking up online relationships:

> 'Ultimately, you have to listen to your instinct, your instinct generally keeps you safe. And it's no different online.'

Notes

1 Fletcher, E (2023) Romance scammers' favorite lies exposed, Federal Trade Commission, 9 February. www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed#ft1 (archived at https://perma.cc/9AUT-XUYP)

2 Ibid

3 Shaw, V (2023) Average loss to romance scams is nearly £12,000, says building society, The Standard, 2 February. www.standard.co.uk/business/money/average-loss-to-romance-scams-is-nearly-ps12-000-says-building-society-b1057424.html (archived at https://perma.cc/L5ZV-HZP4)

4 Fletcher, E (2023) Romance scammers' favorite lies exposed. Federal Trade Commission, 9 February. www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed#ft1 (archived at https://perma.cc/3ZKW-HTKK)

5 Ibid

6 Ibid
7 TSB (2023) Romance scammers break over 60 hearts and wallets every week, warns TSB as Bank reveals fraudsters' cruel tricks, TSB, 2 February. www.tsb.co.uk/news-releases/romance-scammers-break-over-60-hearts-and-wallets-every-week/ (archived at https://perma.cc/26Q4-A393)
8 Sawer, P (2023) Surge in romance fraud sees $316 million taken from victims, The Telegraph, 11 February. www.telegraph.co.uk/news/2023/02/11/surge-romance-fraud-sees-316-million-taken-victims/ (archived at https://perma.cc/S392-2FT9)
9 Fletcher, E (2023) Romance scammers' favorite lies exposed. Federal Trade Commission, 9 February. www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed#ft1 (archived at https://perma.cc/HTG5-MZAX)
10 TSB (2023) Romance scammers break over 60 hearts and wallets every week, warns TSB as Bank reveals fraudsters' cruel tricks, TSB, 2 February. www.tsb.co.uk/news-releases/romance-scammers-break-over-60-hearts-and-wallets-every-week/ (archived at https://perma.cc/V22S-XZ2D)
11 Whitty, M T and Buchanan, T (2016) The online dating romance scam: the psychological impact on victims – both financial and non-financial, *Criminology & Criminal Justice*, 16(2), 176–94. doi.org/10.1177/1748895815603773 (archived at https://perma.cc/8RW6-K882)
12 US Attorney's Office (2023) FBI and partners issue national public safety alert on sextortion schemes, Department of Justice, 19 January. www.justice.gov/usao-sdin/pr/fbi-and-partners-issue-national-public-safety-alert-sextortion-schemes (archived at https://perma.cc/Z84V-VP2Y)

CHAPTER FIVE

Cyber fraud

In July 2018, Alexander Wood was sentenced to seven years in jail, while his accomplice, Muhammed Azhar, was sentenced to nine years. Wood admitted to 11 counts of fraud and one of money laundering. When they were arrested in 2018, the phone which Wood had on his person contained information which tied the pair to crimes against three companies totalling £1.8 million. This was part of a scheme in which he would make phone calls to the finance departments of businesses, claiming he was a senior fraud adviser at their bank, convincing them to make payments to accounts which he and Azhar controlled. When I interviewed Wood, who has turned his life around and now advises the counter-fraud profession, he told me how much deeper the crimes went:

> 'We only got prosecuted for £1.8 million of fraud which was committed over the course of the week before we got nicked

> and the only reason we got done for that is because that was on our phones.
>
> The longer we got away with it – we got away with it for nine months in the end, wrecking businesses, wrecking lives for nine months – we thought we were totally untouchable.
>
> Although they [law enforcement] had loads of complaints, in order to prosecute, they need two separate strands of evidence to mount a charge. So they have to be able to corroborate the complaint with evidence collected from me. They could do that for £1.8 but they think we took at least £50 million in nine months. I don't actually know. All I know is our spending.
>
> Spending it like it's going out of fashion. They [the police, on his arrest] found £8,000 in my jeans. I didn't even know it was there. It was change from a night out, basically.'

When he was arrested, Wood was living in a £2 million townhouse in Camden, London, where police found a stash of Rolexes:

> 'I wasn't living like a criminal hiding in the shadows. I was living a very, very affluent lifestyle.'

What makes a fraudster?

If you have a stereotypical image of a cyber fraudster in mind, Alex Wood is probably not what you're imagining. For one thing, he is incredibly well-spoken with an accent

that would not be out of place in the upper echelons of British society. As it turned out, this accent ended up being part of his criminal endeavours.

When I interviewed Wood, he described an upbringing in a very successful classical musical family. With parents who had highly successful classical music careers, Wood himself played the violin and viola from age four and described a successful youth playing at palaces around Europe (including Buckingham Palace and Windsor Castle), recording professionally and appearing on movie soundtracks. In his early 20s, Wood recounts how his lucrative music career came crashing down with a painful diagnosis of RSI. He regards this as *'very much a turning point in life'* where he should – in hindsight – have taken a different path.

Instead, he started down a road of criminality to maintain the expensive lifestyle that his music career had afforded him:

> 'The first fraud was convincing friends of friends to invest in a completely nonsense, worthless company that I'd set up. And they didn't realize at that point that I'd stopped playing. They saw me as a success with this big flat in Canary Wharf and this nice lifestyle, fast cars and so on. So, it was quite easy. I think I scammed about £50,000 in total, but it was a very crude fraud. It was very, very poorly thought out. I didn't know anything about fraud then. I didn't know that the police would look into my bank accounts and see where it had all gone and trace it and freeze it all. It was quite an easy task for them to unravel it.'

Wood received a three-year sentence for this first offence and went to prison. He – and his family – were shocked,

and he describes what he believes, in hindsight, was *'some form of a breakdown'*. He served his sentence but, when he was released, he found it hard to make an honest living, as he shared with me:

> 'I think a lot of businesses would hire an ex-drug dealer or an ex-violent offender rather than a fraudster because ultimately businesses care about their bottom line. And the idea that somebody might dupe them or steal money is quite worrying. So, I found it really tough [to get a job] and I had a couple of forays into entrepreneurship which didn't go anywhere. I didn't know what the hell I was doing. I drifted about for a few years and did hardly anything, achieved nothing and then eventually found myself homeless.'

Wood describes being evicted from his flat for failing to pay the rent, grabbing a few clothes and his laptop and charger. He ended up at Heathrow Airport, sleeping on a bench and trying to blend in with weary travellers, while he worked out what to do next. He searched online for a hostel, but all were at least twice the price of the £4 he had in his pocket. As he scrolled a hotel booking site online, his search took him from hostels to more-and-more expensive options:

> 'I went to the bottom of the list and there was Claridge's Hotel. And I was looking at it yearningly. I thought, if I could just have that beautiful, warm bed and be in that luxurious suite for a night, you know what I'd give? So then I thought, 'well, f**k it, give it a try'. I set up a fake email account, I didn't really think it through properly, but

I set up a fake email account saying that I was Lord Wood's personal diary secretary. He normally stays at the Ritz. His normal suite's busy these next few days so we'd like him to possibly stay at Claridge's and be happy to talk about making a more permanent arrangement if he's happy with the accommodation.

And I just fired this off thinking nothing would happen. I didn't even have an email signature on it. It was very, very crude, just an Outlook account. The name I chose was something like Quentin Bingham-Smythe. So, it sounded like this super posh diary secretary, potentially plausible.

I thought they were either gonna ignore it or say "eff off". But 10 minutes later the laptop went "ping". And there's this email from Claridge's VIP manager saying, "it will be wonderful to welcome His Grace to stay with us".

I couldn't believe it. I thought it was a joke. Anyway, I emailed back because obviously I realized I can't pay anything. I said we'll have the same payment arrangement he has with the Ritz because I realized they're competitive, they're not gonna check. So, invoice after checkout, 30 days, and they're like, "no problem, that's fine, we'll do that".'

Wood describes being welcomed as a VIP at Claridge's, widely regarded as London's most exclusive hotel. And thus began a five-month period in which Wood hopped between the finest hotels in London masquerading as aristocracy. His scheme came undone – for the first time – when one of the hotels smelled a rat. They Googled his latest

assumed identity – Lord Jamie Spencer, the thirteenth Duke of Marlborough – and discovered that the real Duke of Marlborough was decades older than the man who had checked in. Wood was arrested, interviewed, and bailed late at night. Undeterred, he picked up where he left off, heading back to another luxury London hotel but this time pretending to be an employee of British Airways, knowing that the airline would have a commercial agreement with the biggest hotels in London. He continued for another few months before law enforcement again caught up with him and, because he had offended on bail, he was sentenced to three-and-a-half years in prison.

To some extent, this is where Wood's story really begins. He is sent to Wandsworth Prison for the second time – described by an independent board as 'unsafe and inhumane'[1] – where he met Muhammed Azhar, who had been imprisoned for his involvement in a £113 million fraud, reported at the time to be Britain's biggest (known) fraud.[2] Wood described what happened next:

> 'I met my eventual co-defendant, and we had similar release dates, but he was in for cyber fraud, APP fraud. I knew nothing about APP fraud at this point. It was a Pakistani OCN* and they wanted a Western caller. He identified me as being well-spoken, well-educated, quick thinking and

*Organized Crime Networks (OCNs) are generally sophisticated crime groups with revenues in the millions or billions; with organizations resembling those of legitimate businesses, they operate with strategies and hierarchies, often sharing a common link (geographic, religious or family), their activities often spanning several countries.

said, "you'd be ideal". And he said we know how we got caught, we're not going to do the same thing again. We're going to change it so we won't get caught. He said "you can make millions in a few months. So just come and work with us, do six months' work and then just retire for the rest of your life".

I thought "F**k it, why not?". And I realize that's outrageous. But at the time the default position was that the banks always refunded if the victim could show that they were genuinely duped by somebody phoning with the bank's number and so on. So, I was thinking, "well the victim is going to be the bank then, right?" It felt like a victimless crime. I realized the bank is getting hit and sure, therefore the account holders. But I was thinking "well, banks have budgets for this, they have reasonable loss expectations".

He [Azhar] said, "when you come out, I'll pick you up in a Rolls Royce and we'll go and start work together". And he did. There was a f**king Rolls Royce Phantom there outside Wandsworth when I got released.

Then we started doing this scam together and the first day we stole £100,000 off this law firm. That night or the next night I had my cut delivered. I think I had like £40,000 or £35,000 cash in a suitcase and I was thinking, you know, before I came into prison on this sentence, I had a few pound coins in my pocket and now I've got £30–40k in £50 notes in the suitcase. I was thinking I can do a few of those and just buy my way out of the sh*t I was in.'

The strategy and tactics of a fraud

Wood and Azhar worked together to defraud the finance departments of multiple businesses. Azhar identified the targets, searching for small and successful family businesses: on arrest, his phone had a search history that included '&sons Suffolk', '&sons Yorkshire' and '&sons Kent'.[3] I asked Wood how they identified their targets:

> 'We wanted an easy life, so we wanted to make maximum money with minimum effort and minimum risk of my voice being recorded. We end up targeting the trade sector primarily because we saw them not just as having lots of money and potentially having weak financial resilience, but also being intellectually vulnerable. It turned out to be true.
>
> But then we think "well, hang on, who's targeting the big companies, who's targeting the accountancy firms?". So, we ended up targeting some pretty sophisticated companies and getting massive payments out of them. And it's that overconfidence [that made them vulnerable]. Absolute certainty in their ability to detect it and thinking, "well, I can't be conned".'

Wood made the phone calls to the targets, making them appear legitimate by using caller ID spoofing, in which software and apps are used to falsify the information that appears on caller ID: the software can make the caller ID

text say anything that the actual caller wants it to say. Wood and Azhar made caller ID look like the bank was ringing. Wood claimed he was a senior fraud adviser at their bank contacting them in response to concerns of a computer virus (Wannacry) and associated signs of fraud on their accounts. In this way, he placed himself in a trusted position (calling from the bank), but with a premise that would make the victim panic, clouding their judgement, with the concern of fraud. He was then able to exploit this panic by immediately presenting himself as their rescuer. Peppering the calls with just enough jargon to tread the fine line between bamboozling the victim and simultaneously reassuring them, he built rapport with the victims and created a sense that together they were going to stop the business from being defrauded.

In reality, Wood was using this social engineering pretext to convince the victims to transfer funds to bank accounts that he and Azhar controlled. He told the victims that, to protect the business funds from a virus that was enabling fraudulent activity, they needed to transfer those funds to safe accounts. Wood is very charming. On the calls, snippets of which can be heard in the BBC *File on 4* programme, 'The Anatomy of a Fraud', he adopts an extremely convincing persona:

> 'I was trying to totally dupe the victim that I was phoning from the bank, that they could trust me and that I was authorized to be doing this phone call: I was from the fraud team and I was trying to protect them. I would try and dumb my voice down so I would sound like a lad working in a fraud team of a bank.

> … I just wanted to sound bored and like I was just doing my job: I didn't have to be there, I was going to go home that night and play five-a-side football. So, I'd sort of put myself into this psychological position where I'd imagine I was sitting in this call centre in Essex or something.'[4]

Wood spent a long time on the phone with victims, for example spending two hours on the call, which can be heard in the BBC programme. He explained that this was a tactical decision to ensure that the victim's money was in their control:

> 'I would be keeping the person on the phone until the first layer of mule accounts had been cleared. The more money the company had the longer the call would go on for, because you're instructing more payments to be made.'[5]

In a video shared online by the Metropolitan Police, which shows footage of Wood being arrested, a snippet from one of the calls can be heard. He speaks to the victim of the need to 'suspend the gateway and get you on what's called a diagnostic session'. In a classic social engineering tactic, he uses well-known security measures that banks have implemented to add an extra veneer of authenticity to his patter, reassuring them that 'at no point am I going to ask you for passwords, PINs or codes from your smart card reader'. He mutes the call and can be heard saying to Azhar *'£1.3 [million] gone, I'm gonna buy you a Rolex tomorrow mate'*.[6]

Wood and Azhar covered their tracks by regularly destroying the electronic devices that they used to carry out the crimes. Over time, they became more complacent, but still destroyed their devices every week or so,

beginning their crimes again with fresh phones and laptops. This meant that when they were arrested, the police found smart phones which only contained evidence from the previous week's activities:

> 'The first two frauds, those first two days, I panicked like hell, I was like "Oh my God, I've just stolen £100k, we've got to go and smash the f***ing laptops". We end up smashing this laptop with a cricket bat and throwing it in a river like we were sh*t scared that we were going to get caught. Thinking the police are going to come crashing through the door any minute.
>
> But nothing happened and as time went on, we got six months in, we're saying "we're getting away with this, a lot of money" and it's going on, just becoming more relaxed. And so rather than smashing the laptops and the phones every day, we do it every seven days.
>
> They had all this evidence for seven days' work [when he was arrested].'

Authorized fraud

Wood and Azhar conducted authorized push payment (APP) fraud, which is when criminals manipulate targets into sending payments to bank accounts that they control. APP fraud in the UK rose by 22 per cent in the first half of 2023[7] and research suggests that 78 per cent of these crimes originate online and account for 36 per cent of associated overall losses, whereas 18 per cent take place through telecommunications but account for 44 per cent

of losses.[8] APP takes various forms, generally always involving social engineering – APP scams can be seen in many of the attack types that are covered elsewhere in this book, such as romance fraud, business email compromise, and impersonation and investment scams, often carried out via social media. As well as using social engineering techniques to manipulate their targets, criminals sometimes hack into email and other systems to enable these attacks. The fraudsters use email, social media, text messages and phone calls to deceive their victims into making a payment directly to accounts they control, while the victims are made to believe the money is for legitimate payments to a trusted entity. The increasing ease with which real-time payments can be made is attractive to APP criminals, offering them the ability to quickly move payments through multiple financial accounts, which launders the proceeds in layers and makes the criminal activity harder to identify and trace.

Recovering the funds is very challenging. When the money from fraud ends up in the hands of the criminals, it is quickly siphoned off into layers of mule accounts and often sent overseas. The UK's Contingent Reimbursement Model (CRM) Code is a voluntary agreement which sets out consumer protection standards to reduce APP scams, launched in 2019. UK banks voluntarily opt in to participate, with an aim of providing a more efficient way of streamlining compensation for APP victims.[9] In the UK, known losses due to APP fraud in the first half of 2023 were £239.3 million. Of the total loss, 64 per cent – £152.8 million – was returned to victims, which was an

increase of 13 per cent (£135.6 million) compared to the same time in 2022.[10]

In June 2023, Britain's Payment Systems Regulator (PSR) announced that, from 2024, it will be mandatory for banks and payment companies to reimburse victims of APP within five days, with the cost for reimbursement split evenly between the firm from which payment is sent and the one where it is received. Chris Hemsley, managing director at the PSR, said that *'In delivering this step-change, the UK will be at the forefront of the fight against APP fraud globally'*.[11] In the US, the conditions under which financial firms will reimburse customers or fraud is determined by Regulation E (Reg E) and Reg E does not cover authorized transactions, meaning that banks are not liable to reimburse customers who have been the victim of APP fraud.[12]

APP scams are regarded as the number one fraud threat globally, with losses expected to reach $5.25 billion in the US, UK and India by 2026.[13] However, research from the PSR in the UK found a great deal of disparity between the extent to which banks and other payment service providers reimburse victims of APP, ranging from 10 per cent to 91 per cent of the total value of APP fraud losses being refunded.[14]

Unauthorized fraud

Authorized fraud differs from unauthorized fraud which, by contrast, is when a transfer of money is made from your account without your permission. This can include a

criminal stealing bank cards or financial information, or using stolen identity information. In the first half of 2023, losses due to unauthorized fraud were £340.7 million and, over the same period, UK banks prevented a further £651 million of unauthorized fraud.[15]

Unauthorized fraud includes skimming, when a fraudster uses a skimmer device to steal credit or debit card information. They attach the device to a card reader, for example at ATMs or fuel pumps, and when a customer swipes their payment card, the device captures the data held on the magnetic stripe. They also often use small cameras or overlaid devices to capture PINs as they are entered by customers. They use the stolen information to create counterfeit cards or make fraudulent purchases.

Skimming can facilitate card-not-present (CNP) fraud, when a criminal uses stolen credit card information to make purchases without physically using the card, for example online. The credit or debit card data can also come from data breaches, malware or from a criminal using social engineering to trick the victim into sharing their financial information. Data shows there was a near five times increase in compromised cards due to skimming in the US in 2022, with 161,000 impacted cards identified.[16]

In September 2023, two men were arrested in Australia over an alleged $3.7 million credit card skimming scheme, with police finding the details of more than 1,000 customers alongside card skimming devices and 1,500 blank cards at one home in the suburbs of New South Wales. They also seized $50,000 in cash, electronic devices and designer

products in a second home in the same neighbourhood. Police alleged that the operation was part of an international scheme, believing that the men were members of a Romanian gang who travelled to Australia on false passports with the purpose of conducting the large-scale fraud, which they also carried out in the US, Europe and Asia.[17] The Australian police suspect that at least 3,500 victims were defrauded, with the gang – 'well-known' to law enforcement around the world – targeting busy shopping precincts.[18]

How criminals cash out: money mules

Whether carrying out authorized or unauthorized fraud, criminals often need to 'cash out' their ill-gotten gains in a way which – they hope – does not lead back to them. When conducting fraud of traditional currency (and not relying on the perception of anonymity that comes with cryptocurrency, as explored in Chapter 12), criminals often rely on money mules.*

In Wood's case, it was his associate, Azhar, who was responsible for managing the cashing out element of their operation. When I interviewed Wood, he described to me how they used a network of money mules around the UK, convincing the victims he spoke to on the phone to transfer their business funds to 'safe accounts' when in fact they

*A money mule is a person who transfers or moves illegally acquired money on behalf of someone else.

were transferring it to money mule accounts under the control of Wood and Azhar:

> 'Depending on the size of the job that we had to clear, say there's £1,000,000, he [Azhar] would then give me the details for 10 commercial accounts to put 100k in each one, and then once that hit those accounts, he'd then siphon it out to a whole string of student mule accounts. From there it would be cashed out because you can't go into a branch and withdraw £100k from a commercial account, but you can withdraw £5k from a student account quite easily.
>
> You have these guys who would sit in coffee shops in the high streets of Birmingham, Ilford or Hounslow, sitting with a pocket full of debit cards waiting for a text to say "right, £5k's on this card" and then they go into the branch.'

As part of his work now, Wood focuses on raising awareness of fraud and advocating ways to improve anti-fraud controls – for him, one of the key linchpins is tackling the use of money mules:

> 'How can we disrupt this? How can we aggressively disrupt this with the same level of intricacy that the fraudsters are deploying?
>
> You can't say fraud is really bad, you've got to stop. So you can't change the fraud being committed. The only thing you can viably change is the methods by which fraudsters can realize their funds and cash out. And so that's why I focus quite a lot on mule accounts and how to disrupt mule activity.'

In December 2022, law enforcement from 25 countries – supported by Europol, Eurojust, Interpol and the European Banking Federation (EBF) – announced the biggest international operation of its kind to tackle *'one of the most important enablers of money laundering: money mules and their recruiters'*.[19] This international operation identified 222 recruiters and 8,755 money mules; they made 2,469 arrests and intercepted nearly €18 million (over $19 million or £15.5 million).[20]

Money mules are recruited in different ways. Some know that they are supporting criminal activity and agree to be part of it to take a commission. Others are unknowingly manipulated when they are offered a way to make easy money with little demand or detail, or by someone who claims they need help moving cash and cannot use their own account, or by romance fraud.

In 2014, 74-year-old Glenda Seim met the love of her life online. He told her he was a US citizen working in Nigeria, needing money to help his business and enable him to leave Nigeria. He sent her electronic devices to pawn and then had her open personal and business bank accounts, before sending her cheques and having money deposited into the accounts. Seim had unwittingly become a money mule. In 2015, bank employees, the police and US federal agents told her it was a scam and that if she did not stop complying, she would face jail. Her online romancer convinced her otherwise. She received multiple warnings over five years and then, in November 2021 – when Seim was 81 years old – she pleaded guilty to two federal crimes and collaborated with authorities on a public service announcement to raise awareness of money mules, produced by the FBI and other US agencies.[21]

The impact of fraud

In the week before their arrest, Wood and Azhar defrauded three family businesses out of £1.8 million, convincing the victims that they had been infected with the Wannacry virus. One of the companies lost nearly £1.3 million and, overall, police believed they had stolen more than £50 million.[22]

Beyond the financial losses, being a victim of a scam can take a huge toll on someone's mental and physical health. Victims can often feel ashamed, angry and distressed. People can blame themselves and become preoccupied that it could happen to them again and can lose confidence. Being a victim of fraud can leave people with symptoms including severe anxiety, sleep disorders, depression, and post-traumatic stress disorder (PTSD).[23] There are reports of victims self-harming and dying by suicide.[24]

Wood describes a mindset that largely compartmentalized his actions and the victims, not really thinking about the people on the other end of the phone, convincing himself that it was a 'victimless' crime. There was only one call which he told me stuck in his mind, where the victim sounded like his mum, thanking him and calling him *'my dear'*. Otherwise, it was only when he had been arrested that the impact of his actions became clear to him:

> 'With fraud, the only time you understand the devastation you've caused is when it goes to court or when you get nicked and you start to hear victim impact statements. And it's then that you understand that what you've told yourself is victimless has had a profound effect on people's lives and health, their relationships and well-being.

> We were only prosecuted for three frauds, three victims. And we must have made hundreds of phone calls. And out of those three, one had a stroke. So I just dread to think.'

The victim impact statements from Wood and Azhar's crimes disabuse any notion that fraud is 'victimless'. One victim of Wood and Azhar spoke of *'the day my world fell apart'*; another shared the impact that the experience had on their family: *'my brother has been in a downward spiral of depression that resulted in him being hospitalized'* and a third described having to close down part of the business, with 13 people losing their jobs.[25] One victim described how a family member had a mini-stroke and turned to alcohol to numb the emotional fallout, adding how the pressure and stress had damaged his marriage.[26]

In July 2018, Azhar was sentenced to nine years in prison after pleading guilty to eight counts of fraud and one of money laundering. Wood plead guilty to eleven counts of fraud and one of money laundering and was sentenced to seven years.[27] He was released in early 2022 and now delivers keynote speaking and consultation to the public sector and financial institutions, to raise awareness of the dangers and risks of fraud.

Wood spoke to me of the regret he now feels:

> 'If I'd known then [when Azhar was first approaching him] that people, when hit with this type of fraud, kill themselves, or in my case suffer strokes, then I obviously would have run a mile.
>
> I can never undo the pain that I've caused these people, and I don't want them to ever accept my apology or think I'm a

good guy or what I'm doing is having a positive impact in any way. But if we can just prevent one more person from killing themselves or having a stroke, then that's work well done.'

Fighting fraud: how to stay safe

Fraud accounts for 40 per cent of crime in the UK and receives less than 1 per cent of police resource.[28] In the US, data from the Federal Trade Commission shows consumers reported losing $8.8 billion to fraud in 2022, an increase of more than 30 per cent over the previous year.[29] It is clear that much more needs to be done to protect people from fraud.

In the UK, StopScams is an industry-led collaboration of banking, telecoms and technology businesses, with 22 members including household names such as Amazon, Google and VISA. In 2021, they launched the 159 phone service, with 16 banks signed up. This service enables a customer who is on the phone with someone claiming to be their bank to hang up and call 159 to be connected directly with their bank and assured of their identity.[30]

Some banks implement measures to improve customers' ability to verify legitimate calls. In 2018, Barclays became the first UK bank to introduce a verification feature which allows Barclays customers to receive an alert in their app or online banking to confirm the caller's identity. So, if you are a Barclays customer and receive a call purporting to be from them, you can request confirmation via this verification feature, which confirms the call and displays the name

of the person at Barclays you are speaking with. In September 2023, Monzo bank in the UK launched a similar feature. Wood's advice is that *'banks would be very wise to adopt that across the board'*. Beyond that, he cautions that *'the bank should never call you unless they pre-arrange to call'*.

Being aware of fraudsters' tactics and the increasing sophistication of some of their methods is incredibly important. Banks will never call and ask you to send money to another account, make a payment, ask for your card PIN or personal information, or ask you to install software on your computer or devices. If you receive a call that is allegedly from your bank, hang up and call them back on the number from your bank card, bank statement or website (or, if you are in the UK and your bank is signed up to the 159 service, you can use that). If you receive an email asking for information or for you to make a payment, rather than replying or clicking any links in the email, call the supposed sender on a number you know to be legitimate. Being cautious of unexpected requests to make payments – whether via email, phone, text messages or another means – is important, so always verify the legitimacy of the request via another communication channel.

Be alert to red flags of social engineering (covered in greater detail in Chapter 1) as criminals carrying out authorized fraud often try to make their targets feel panicked, flattered, hurried or worried. If you feel your emotions rising and you are being pressured into taking an action – such as making a payment – slow down and take a step back. Verify who you are communicating with. Criminals will often use current events to make their social

engineering attempts more persuasive, for example the way Wood and Azhar used the Wannacry virus (which had made headline news around the world). Over the last few years, criminals have used the Covid-19 pandemic, the cost-of-living crisis and global conflict.

Avoid unauthorized fraud by checking card readers for indications of skimming devices, inspecting the device for any signs of tampering and covering the keypad when entering your PIN. Personally, if I am using an ATM, before I put my card in, I hold the card reader and give it a pull to check that it is not loose, giving the keypad a prod to check that it is also secure. When using an ATM, it is generally safer to use those inside the bank rather than on the street, if possible, as those inside the bank are less likely to have been tampered with.

Regularly check bank statements to audit your transactions and identify if any are suspicious or unknown to you and contact your bank if this is the case. In general, credit cards offer better fraud protection over debit cards. Using contactless payment (aka tap-to-pay) is more secure because each transaction uses an encrypted, unique, one-time digital code to secure the communication between the card reader and your card. This code does not include your personal or financial information, so it prevents fraudsters from cloning the card.

Contactless fraud does happen, but it is currently limited and unsophisticated. In 2022, UK figures show a total loss of £726.9 million through unauthorized card fraud and of this only £34.9 million is tied to contactless payment fraud, out of a total of £231 billion contactless transactions.[31] Although the percentage is small, that is still £34.9 million

lost to criminals. To protect against contactless fraud, we can keep bank cards safe and report any lost or stolen cards to the bank straight away, because this fraud generally involves criminals finding or stealing contactless cards and using them to make payments up to the limit. Making contactless payments with a mobile phone or smart watch allows for the added security of using face-ID, fingerprint or passcodes, so this can allow you to keep your card safe at home while making payments via smart devices.

Fraud is a huge problem, and has been made ever more so with advancements in connected technology, which criminals can use to research and reach victims with ease, all while impersonating trusted entities and attempting to obscure their tracks. We are getting better at finding ways to disrupt fraudulent activity and use technology to safeguard people and businesses, but it is clear that much more needs to be done. The financial impact of fraud is devastating enough – on a personal, organizational, social and economic level – but the emotional and psychological impact on some victims is heart-wrenching. As criminals continue to evolve their strategies and tactics, we must be aware of the playbooks for these crimes and spread that awareness, especially among the more vulnerable people and companies in our communities.

Notes

1 Warren, J (2023) Wandsworth prison unsafe and inhumane – watchdog report, BBC News, 11 October. www.bbc.com/news/uk-england-london-67065800 (archived at https://perma.cc/6792-3FK6)

2 Green, J (2018) Fraudster who once posed as the Duke of Marlborough and swindled £1.7 million from small businesses is jailed for seven years, Mail Online, 13 July. www.dailymail.co.uk/news/article-5950729/Con-artist-posed-Duke-Marlborough-jailed-seven-years.html (archived at https://perma.cc/QP9C-9S79)
3 www.parikiaki.com/2018/07/two-men-defrauded-three-family-run-businesses-out-of-nearly-2-million/ (archived at https://perma.cc/7PNU-ZGQW)
4 BBC Radio 4 (2023) The Anatomy of a Fraud, File on 4, 29 October. www.bbc.co.uk/programmes/m001rqrl (archived at https://perma.cc/X5ER-KZZN)
5 Ibid
6 Metropolitan Police Service (2018) Officers catch fraudsters who conned family businesses out of £2m. www.facebook.com/metpoliceuk/videos/officers-catch-fraudsters-who-conned-family-businesses-out-of-2m/1882892648434365/ (archived at https://perma.cc/YU8T-4952)
7 Muir, M (2023) Push payment fraud cases jump 22%, Financial Times, 24 October. www.ft.com/content/1884aa46-c9a2-4dcb-9565-d6e743434d19 (archived at https://perma.cc/8ECY-EV29)
8 UK Finance (2023) Over 1.2 billion stolen through fraud in 2022, with nearly 80 per cent of APP fraud cases starting online, UK Finance, 11 April. www.ukfinance.org.uk/news-and-insight/press-release/over-ps12-billion-stolen-through-fraud-in-2022-nearly-80-cent-app (archived at https://perma.cc/84HQ-F2UJ)
9 Lending Standards Board, the Contingent Reimbursement Model Code (CRM Code). www.lendingstandardsboard.org.uk/crm-code/#firms-that-have-signed-up-to-the-code (archived at https://perma.cc/FB75-MZFJ)
10 UK Finance (2023) Over 1.2 billion stolen through fraud in 2022, with nearly 80 per cent of APP fraud cases starting online, UK Finance, 11 April. www.ukfinance.org.uk/news-and-insight/press-release/over-ps12-billion-stolen-through-fraud-in-2022-nearly-80-cent-app (archived at https://perma.cc/DYT7-YJ86)
11 Clark, J (2023) UK banks to reimburse fraud victims under new rules, regulator confirms, The Guardian, 7 June. www.theguardian.com/money/2023/jun/07/uk-banks-to-reimburse-victims-under-new-rules-regulator-confirms (archived at https://perma.cc/2NRN-36NS)

12 Biger-Levin, A (2023) Utilizing the UK Contingent Reimbursement Model to address losses in online scams, Thomson Reuters, 3 April. www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/uk-contingent-reimbursement-model/ (archived at https://perma.cc/3QWK-ULRX)
13 ACI Worldwide (2023) Prime time for real-time global payments report. insiderealtime.aciworldwide.com/prime-time-report-23 (archived at https://perma.cc/LJ22-7W72)
14 Muncaster, P (2023) Regulator reveals large disparity in APP fraud reimbursement, Infosecurity Magazine, 31 October. www.infosecurity-magazine.com/news/regulator-large-disparity-app/ (archived at https://perma.cc/KF35-H93N)
15 UK Finance (2023) Over 1.2 billion stolen through fraud in 2022, with nearly 80 per cent of APP fraud cases starting online, UK Finance, 11 April. www.ukfinance.org.uk/news-and-insight/press-release/over-ps12-billion-stolen-through-fraud-in-2022-nearly-80-cent-app (archived at https://perma.cc/XB6S-AK4V)
16 Cobb, D (2023) US card skimming grew nearly 5x in 2022, new FICO data shows, FICO Blog, 16 February. www.fico.com/blogs/us-card-skimming-grew-nearly-5x-2022-new-fico-data-shows (archived at https://perma.cc/F8PZ-VAGX)
17 Goodwin, S T (2023) Romanian duo arrested in Sydney after alleged $3.7m credit card skimming scheme, ABC News, 27 September. www.abc.net.au/news/2023-09-28/nsw-credit-card-skimming-scheme-charged/102912052 (archived at https://perma.cc/7NU4-7ZAV)
18 Meacham, S (2023) Two men charged over alleged $3.75m card skimming scheme, 9 News, 28 September. www.9news.com.au/national/nsw-crime-credit-card-skimming-scheme-3-million-dollars-two-men-charged/f54170a6-99b0-4208-aa72-197fa2d7567a (archived at https://perma.cc/TR56-KKEY)
19 Europol (2022) 2,469 money mules arrested in worldwide crackdown against money laundering, Europol, 5 December. www.europol.europa.eu/media-press/newsroom/news/2-469-money-mules-arrested-in-worldwide-crackdown-against-money-laundering
20 Ibid

21 FBI (2021) Victim of romance scam who became money mule tells her story. www.fbi.gov/video-repository/sl-money-mule-psa-110221.mp4/view (archived at https://perma.cc/NZ7V-3NKN)
22 Atkins, C (2023) Prison turned my cellmate into a £50m fraudster. Behind bars, it's like crime school, iNews, 8 September. inews.co.uk/inews-lifestyle/prison-turned-friend-fraudster-2598237 (archived at https://perma.cc/9PDE-HLFW)
23 Ianzito, C (2022) Many victims struggle with mental health in scams, Aftermath AARP, 15 December. www.aarp.org/money/scams-fraud/info-2022/mental-health-impact.html (archived at https://perma.cc/7DE6-65CL)
24 Sun, D (2023) The painful cost of scams: suicide and self-harm, The Straits Times, 14 January. www.straitstimes.com/singapore/the-painful-cost-of-scams-suicide-and-self-harm (archived at https://perma.cc/6FWW-NWCP)
25 Parikiaki (2018) Two men defrauded three family-run businesses out of nearly £2 million, Parikiaki, 14 July. www.parikiaki.com/2018/07/two-men-defrauded-three-family-run-businesses-out-of-nearly-2-million/ (archived at https://perma.cc/JJ3M-DLL3)
26 Green, J (2018) Fraudster who once posed as the Duke of Marlborough and swindled £1.7 million from small businesses is jailed for seven years, Mail Online, 13 July. www.dailymail.co.uk/news/article-5950729/Con-artist-posed-Duke-Marlborough-jailed-seven-years.html (archived at https://perma.cc/QNH7-CH2G)
27 Ibid
28 HM Government (2023) Fraud strategy: stopping scams and protecting the public. assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1154660/Fraud_Strategy_2023.pdf (archived at https://perma.cc/93FZ-GZXY)
29 Federal Trade Commission (2023) New FTC data shows consumers reported losing nearly $8.8 billion to scams in 2022, FTC, 23 February. www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022 (archived at https://perma.cc/D66P-D7WQ)

30 Stop Scams UK, Stop. Hang up. Call 159. stopscamsuk.org.uk/159 (archived at https://perma.cc/7PNU-ZGQW)
31 Cox, M (2023) Contactless payment fraud – A sleeping lion in a trillion-pound market, FICO, 8 August. www.fico.com/blogs/contactless-payments-fraud (archived at https://perma.cc/KGU4-SDJC)

CHAPTER SIX

Identity fraud

In 2005, Sandra Estok and her family were relocated by her employer from Venezuela to the American mid-west. After settling in the United States and, in her words, '*surviving her first winter*', Estok went for a trip back to South America to visit her mother. After a wonderful family reunion, Estok returned to the States and her plane landed in Miami. She did not think much of it when Homeland Security Officers started boarding the plane, safe in the knowledge that she had her passport and visa. Until, the next thing she knew, she was suddenly the only passenger being marched off the plane by those officers. She was led into a room, unable to make a phone call, and in the dark as to what was happening to her. She worried about making her connecting flight to Chicago, where her husband was waiting for her. After ten hours of confusion,

uncertainty and waiting, her passport was handed back to her with a big, red stamp on the visa: 'REVOKED'.

The whole room gasped when Estok shared that final detail above: I was at a cyber security conference with hundreds of cyber security professionals, hearing her tell her story on stage.[1] Estok went on to explain that she and her husband were forced to leave their American life behind and return to Venezuela. With the support of her employer at the time, she headed to the Embassy to resolve whatever the issue was, where she found herself confronted with questions which made no sense to her. A diplomatic security officer asked her why she went to China, who she knew in China, who her contact was. But, Estok had never been to China.

Estok's identity had been stolen and was being used by a criminal in China, smuggling women into the United States. For the following six years, she had to prove she was the real Sandra Estok, over and over again.

It is hard to even imagine being in this situation. After hearing Estok's powerful, sobering and – ultimately – inspiring presentation, I caught up with her to see if she would share more about her experience.

The impact of identity fraud on victims

I asked Estok to describe the impact that being a victim of identity theft had on her life:

> 'Circumstances forced my family and me to abruptly leave the US and return to Venezuela to secure a new work visa

after mine was suddenly revoked. The uncertainty of not knowing why compounded the stress. The subsequent revelation at the American Embassy in Caracas – that a criminal was using my identity to smuggle women into the US – left me shocked. What followed went beyond anything I could have imagined.

Those six long years were an absolute nightmare. Being constantly misunderstood, subjected to scrutiny, and doubted I was the real me over and over was more than just a hurdle; it became a deeply personal battle. This phase eroded my self-esteem, shook my faith in the system, threatened my marriage and career, and weighed heavily on my health and mental well-being.

We all assume identity theft won't happen to us... until it does. In my case this adversity ignited a passion within me to prevent others from learning this the hard way. We must be mindful, stay alert, and value our precious personal data.'

Estok's experience is scary enough, but it becomes scarier when we understand the scale of identity theft and fraud. The United States Department of Justice reported that, in 2021, 23.9 million people (9 per cent of US residents aged 16 or over) were victims of identity theft during the previous 12 months. Of those, 59 per cent had financial losses, which totalled $16.4 billion that year. That is a lot of money going into the hands of criminals. Victims do not just experience financial losses, but can experience an emotional impact too: 10 per cent of the victims in the Department of Justice report were severely distressed because of the crime. The report goes on to highlight that

22 per cent of people in the United States – more than 1 in 5 – had experienced identity theft in their lifetime.[2]

This bleak picture is not restricted to the United States. Research in the UK shows that 24 per cent of UK citizens have been a victim of identity fraud, which is the highest figure in Europe. 63 per cent of victims suffered from financial loss and on average, it takes UK victims 7 months to realize they have been a victim and more than three more months to resolve the situation.[3] Sometimes, as in the case of Sandra Estok, these two phases can take many years.

Victims of identity fraud can be left dealing with the fallout, with companies and debt collectors holding them responsible for purchases and financial agreements made fraudulently in their name. In May 2023, Dean Allen discovered that he had been a victim of identity fraud with his details used to take out three mobile phone contracts with the UK telecom company O2. Allen reported the crime to the police and the UK's Action Fraud but continued to receive default notices, saying that it took 55 emails with O2 and other bodies to sort out the issue. Allen, who described how he 'dreaded coming home', had his case upheld by the UK's Communications Ombudsman after five months, with O2 apologizing and updating his credit file so that he was no longer held accountable for crimes conducted in his name.[4]

Being a victim of cyber crime and identity theft can lead to people feeling paralyzed, ashamed, traumatized and undermined. The psychological impact of identity theft is often overlooked, with more focus on the financial

ramifications for victims. However, the emotional impact can be very challenging. Research from the Identity Theft Resource Centre suggests that victims are finding the psychological impact of identity theft increasingly difficult to deal with: 87 per cent of victims reported that the incident left them feeling worried or anxious, 63 per cent sad or depressed and – most concerning of all – the number of those contemplating suicide as a result of the crime rose from 8 per cent in 2020 to 16 per cent in 2022.[5]

The scale of identity theft and identity fraud

Identity fraud encompasses identity theft: identity theft is the theft of personal or financial information and identity fraud is the use of that stolen information. Identity fraud is the use of false identifiers (false or fraudulent documents) or a stolen identity (identity theft) to commit a crime. It often begins with a 'breeder document', such as a driver's licence or birth certificate, which criminals obtain or create using stolen or fabricated identification data, such as date of birth and government identity numbers (such as passport number or Social Security number). This 'breeder document' is then used to create other documents to enable the creation of a credible identity, providing a criminal with an identity they can use to get credit cards, set up bank accounts, access information, apply for mortgages, make purchases and much more. They can use this identity to commit criminal activity, such as human smuggling (as in Estok's case), human trafficking, money muling, drug trafficking, cyber crime, terrorism and more.

In the UK, identity fraud hit an all-time high in 2022, with cases increasing by a quarter that year. Over 277,000 cases of identity fraud were recorded in 2022, which is the highest number of cases ever recorded.[6] Most victims of identity theft are over 31 years of age and statistics also show that there has been a significant rise in victims over 61 years of age.[7]

Although older adults are the most common target of identity theft, people of all ages can become victims, including children. Children's details, such as their name and government-issued identification such as Social Security number, are attractive to cyber criminals because the crime has more potential to go undetected for a longer period, for example until the child is old enough to apply for their first loan or credit card. Research suggests that one million children in the United States were the victim of identity theft in 2017.[8]

The tactics of identity fraudsters

As well as targeting the identities of children to use in identity fraud, criminals also sadly target the personal information of people who have died, knowing that their credit is less likely to be monitored by relatives left behind. This form of identity fraud can compound grief and stress for grieving relatives, who often only become aware that the crime has been committed when creditors try to collect. Unfortunately, fraudsters often use publicly available information – such as news articles, published obituaries or dedications posted on social media – to begin this crime.

They may then impersonate a government official or family member to glean more information about the individual. In February 2023, Katrina Pierce was sentenced to just over five years in prison after allegedly fraudulently obtaining the identities of deceased children and adults and using the stolen identities to steal over $45,000 of government funds. Pierce is reported to have acquired over 36 death certificates for murder victims in the US (ranging from 2 to 22 years) after pretending to be related to them. She is then alleged to have used the stolen identifiers (including dates of birth and Social Security numbers) to file for pandemic stimulus payments and tax refunds.[9] In other cases, criminals may use the personal information of deceased people to apply for loans, open credit cards, buy electronic goods and more.

When details of children or those who have died are used in identity fraud, they are often combined with fake information to form a 'synthetic identity'. Research suggests that the fastest growing financial crime in the United States is synthetic identity fraud, in which real (generally stolen) and fake identity information is combined by criminals to fraudulently create accounts or make purchases.[10] The scale of these crimes can be eye-opening. In one case, a group of five men in Florida, USA, established 700 synthetic identities by combining stolen information such as Social Security numbers with fake identity information, including false names and dates of birth. In 2020, this group committed multiple crimes with these synthetic identities (and shell companies established with the fake details), including defrauding banks and stealing over $100 million from Covid-19 relief programmes.[11]

Sometimes, identity theft and fraud can be perpetrated closer to home. In June 2023, Kevin J Thompson was reportedly arrested on charges related to the impersonation of former NFL player Earl Thomas III, including identity theft, forgery, money laundering, credit card fraud, computer fraud and bank fraud. It is alleged that Thompson was in a relationship with Thomas' ex-wife and used a driver's licence with his own photograph alongside the NFL player's personal information to carry out the crimes. He is alleged to have used this fraudulent ID to open a bank account in Thomas' name and move money from Thomas' account into the account which he had opened, apparently to the tune of at least $700,000; he is also alleged to have transferred ownership of several of Thomas' vehicles before selling them and keeping the proceeds, bringing the total sum that he is accused of defrauding to almost $2 million.[12]

The role and impact of identity fraud cannot be underestimated: it is a common component of most criminal activity. For an individual, the impact can range from being a nuisance (for example, having to call the bank and cancel fraudulent bank charges) to almost ruining someone's life.

Cyber crime both feeds and is fed by identity fraud. Identity crimes are the most frequently committed criminal offences except for property crimes, being committed more than all violent crimes combined.[13] Research also shows that most identity fraud occurs online, with 86 per cent being committed through online channels.[14] There are multiple ways in which criminals steal personal and financial data from people online, to use in identity fraud. This includes social engineering, in which the fraudsters

manipulate people into sharing personal and financial information, believing they are doing so with a trusted individual or organization. This can include everything from impersonating your bank in a phone call to posing as a love interest and building up trust over internet chats to social media scams such as false job advertisements and ambassador scams. When companies are hacked or websites are breached, the personal and financial data of customers is often stolen and used in identity fraud, either by the criminals who perpetrated the original attack or bought on the dark web by other criminal groups who use it – or both. Malicious software (malware) can be used by criminals to take over your devices and access personal and financial information on your phone or computer, or in your online accounts. Card skimming is another method criminals use to steal financial data, using skimming devices that they attach to card readers to steal debit and credit card data and make copies of your card.

Identity fraud and cyber crime

Criminals also use identity theft as a cog in the machine of cyber crime, for example stealing the credentials of an individual and using them to gain access to their company or personal accounts, going on to steal further information, steal funds or infect the system with malicious software (see Chapter 10 on ransomware). Criminals use identity fraud for all sorts of purposes, including purchasing goods, getting credit cards, opening accounts such as phone accounts, taking out loans, carrying out tax fraud, applying

for government benefits and loans, and more. Criminals can use personal and financial data that they steal to carry out more crime under a false name and with false details, as in Estok's case with a criminal in China using her details to smuggle women into the United States. Criminals use the data of identity theft victims in many crimes, for example using stolen credit card data to set up scam sites with the victim's information. This makes it harder for law enforcement to identify the true perpetrators, with the digital finger pointing at the identity theft victim. This is one reason why it is so important to be alert to the signs of identity theft and report it to the authorities.

I asked Estok if she knows how her identity was stolen, and this is what she shared:

> 'I was not as careful with my personal information as I am now. That does not mean I was not smart, or that I didn't care about protecting my information or family, I just did not know exactly how to do it.
>
> In hindsight, I was unaware. I didn't pay enough attention to how I managed sensitive information or stayed alert when asked for personal documents. I would casually provide my passport, credit card, etc. without considering the implications. I entered data on questionable websites and freely handed over identification when requested without thinking twice. It pains me, but this lack of mindfulness left me susceptible to theft.'

We can all be distracted, trying to multitask through our busy days, which can be a factor in oversharing or being socially engineered. After her experience with identity

theft, mindfulness is central to Estok's work now in cyber security:

> 'In our fast-paced world, it is easy to get caught up in the whirlwind of tasks and responsibilities. Before I knew it, I was juggling so many balls that I dropped the one labelled "personal security". This eye-opening episode taught me that we cannot let life's chaos blind us to the basics. It's all about keeping ourselves and our loved ones safe so that we can have peace of mind online and offline.'

Avoiding identity theft

As a victim of identity theft who has now become an award-winning author, podcast host and international keynote speaker on the topic of cyber security, I asked Estok what advice she has to be more secure online:

> 'There are three fundamental choices to be more secure online.
>
> First, "Be intentional" in everything you do. Act on purpose, whether sharing and connecting with your friends online, sharing personal information, and more.
>
> Second, "Be aware", cultivate cyber knowledge and integrate it with every aspect of your life, and notice what happens to you physically, mentally and spiritually. Cyber knowledge helps you regain your power and make the changes you need so you will be in charge of your cyber safety.
>
> And lastly, "Be mindful". Be fully present in all you do whether online or offline. Pay attention to your surroundings

> because when we are more present, we make better decisions. A simple way to be mindful is to pause and breathe before your next click.'

This focus on mindset is so important, because cyber criminals continuously evolve their tactics to evade our defences. As I covered in Chapter 1, criminals have adapted to new measures by moving beyond phishing emails to phishing messages, phone calls, and phishing over social media and QR codes. We also see this with the use of deepfake technology in social engineering, as I'll explore in Chapter 13. Having strong situational awareness and being mindful with our approach to technology and information helps us take a more strategic approach.

With this mindset, there are practical steps we can all take. First, reflecting on the statistic that it takes the average victim seven months to know their identity has been stolen,[15] it is important to be aware of the signs of identity theft. These include being alert to unexpected activity with financial services, such as transactions on bank statements that you do not recognize, unforeseen issues with credit or receiving unexpected bills. Look out for issues with paperwork, too. If you receive notice that you unexpectedly owe tax or have apparently filed multiple tax returns, these would be red flags, as would any unanticipated changes to your personal information (such as your address) on accounts.

Being aware of the signs of identity theft, such as those listed above, is important so that we can spot if something untoward is taking place. There are also proactive steps we

can take to minimize the dangers of being a victim of identity theft:

1 Protect electronic information by using strong PINs or passcodes on devices and using strong passwords and two-factor authentication on all online accounts (see Chapter 2); install updates on devices as soon as they become available (see Chapter 3) and wipe electronic devices before selling or disposing of them.
2 Protect hard copies of data by keeping all important documents in a safe place and running them through a cross-shredder before disposing of them.
3 Be alert to social engineering and be mindful of information you share online, for example on social media.
4 Regularly review your bank statements, credit card bills and credit score for anything unusual and consider credit monitoring and freezing, if this is available to you.
5 Report lost or stolen items immediately, such as your government ID, passport, wallet, and devices, as the information they contain could be used to steal your identity. If you think you may have been a victim of identity theft, contact law enforcement, credit agencies and your bank, keeping a record of who you communicate with and tracking names, dates and information exchanged as much as possible.

Notes

1 Estok, S (2023) Elevate your security awareness program: harnessing the power of mindfulness, SANS Security Awareness, 11 October 2023. youtu.be/h097LepwCOQ?si=SYl6pmDIi9Y7hqBF (archived at https://perma.cc/67TY-3EBM)

2 Stop ID fraud, Consumer facts. www.stop-idfraud.co.uk/the-facts/the-consumer/ (archived at https://perma.cc/6BGW-D8J7)
3 Elahi, A S (2023) O2 phone contract scam: Colchester victim worried bailiffs would come, BBC News, 13 November. www.bbc.com/news/uk-england-essex-67380001 (archived at https://perma.cc/LT96-FAWZ)
4 Stop ID FRuad Consumer Facts. www.stop-idfraud.co.uk/the-facts/the-consumer/ (archived at https:// perma.cc/3DA9-VGQB)
5 Flores, S and Pasillas, C (2023) Identity theft can harm your mental health as well as your credit, NBC San Diego, 23 August. www.nbcsandiego.com/nbc-7-responds-2/identity-theft-can-harm-your-mental-health-as-well-as-your-credit/3291243/ (archived at https://perma.cc/MY39-LPAV)
6 Cifas (2023) Fraudscape 2023. www.fraudscape.co.uk (archived at https://perma.cc/MJ75-7S4N)
7 Ibid
8 The Federal Reserve (2019) Synthetic identity fraud in the U.S. payment system: a review of causes and contributing factors. fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf (archived at https://perma.cc/AW3V-LA3M)
9 Chung, C (2023) Woman used identities of dead people to defraud US, officials say. The New York Times, 12 February. www.nytimes.com/2023/02/12/us/tax-fraud-dead-chicago.html (archived at https://perma.cc/N4Q5-5KWS)
10 Mastercard Identity (2023) Uncovering synthetic identity theft with real-life cases and examples. https://ekata.com/blog/uncovering-synthetic-identity-theft-with-real-life-cases-and-examples/ (archived at https://perma.cc/HB5W-SZGC)
11 US Department of Justice (2022) South Florida US Attorney's Office to lead COVID-19 fraud strike force team against pandemic relief fraud, US Department of Justice, 15 September. www.justice.gov/usao-sdfl/pr/south-florida-us-attorney-s-office-lead-covid-19-fraud-strike-force-team-against (archived at https://perma.cc/45UL-UJH4)

12 Hunter, M (2023) New Orleans man posed as NFL player Earl Thomas in $1.9M identity theft scheme, JPSO says. Nola.com, 7 November. www.nola.com/news/jefferson_parish/kevin-thompson-earl-thomas-nfl-arrested-jpso/article_eb194444-7daf-11ee-a75e-b7b9f4926128.html (archived at https://perma.cc/Q7M9-JSHH)
13 Identity Theft Resource Center (2023) 2023 Consumer impact report. www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf (archived at https://perma.cc/75FM-J8JU)
14 Cifas (2023) Fraudscape 2023. www.fraudscape.co.uk (archived at https://perma.cc/PP9E-6QD8)
15 Stop ID fraud (Consumer Facts. www.stop-idfraud.co.uk/the-facts/the-consumer/ (archived at https://perma.cc/3DA9-VGQB)

CHAPTER SEVEN

Social media scams

> 'I will likely never get over the feeling of humiliation and embarrassment at being so easily conned when I thought I was too clever to be conned in this way.'[1]

Valerie, 73 years, had received a WhatsApp message from one of her sons, letting her know that he was using a new phone number. As he runs his own small business, it was not unusual for him to borrow money from her, so when he asked her to transfer £2,000, she was not too surprised.

Nigel Gammon, 77, received a similar message, apparently from his son Jock. They regularly chat on WhatsApp, so when Nigel received a message from Jock saying that his phone had broken and he was using a temporary number, Nigel did not think much of it. Jock needed his

father's help with an urgent payment that had to be made – could his father send him photos of the front and back of his credit card? Eager to help, with his son having recently moved overseas, Nigel sent the photos and Jock replied 'Thank you a lot dad' with a heart emoji. By the time Nigel discovered that he had been communicating with a criminal, and not Jock, over $27,000 had been stolen from his account. So far, only $9,000 has been recovered.[2]

Both Valerie and Nigel were victims of a WhatsApp scam that has swept the messaging platform (and other services, such as texts) in recent years. It is known as the 'Hi Mum, Hi Dad' scam, a form of impersonation fraud. Valerie and Nigel are far from being alone in becoming victims of this: in under five months in 2022, UK's Action Fraud received 1,235 reports of this scam, with a total financial loss of £1.5 million.[3] Scammers are very personable in their conversations with the targets, building rapport and using emoji to make it seem like they really are a family member, while preying on parents' common keenness to help their children. Some cases indicate that they have used social media to perform some reconnaissance on the target, but often they simply begin 'Hi Mum' or 'Hi Dad' and go from there.

In some instances, such as Valerie's, banks refund the victims of these scams. She felt that her bank treated her fairly and refunded the loss. In other cases, they refuse and argue that the victim should have taken more steps to verify the request was genuine.[4] These WhatsApp scams are a form of APP, which we explored in Chapter 5, with real-time faster payments that make it harder to get the money back.

Fake people

Criminals do not just use WhatsApp for their widespread impersonation scams, which can take many different forms, over different platforms and affect people of all ages.

'Is this you?! Or you been hacked'.[5] When Bronte Gosling received this message from one of her contacts, it was the first clue that something was amiss. The messages her contacts had received were not from Bronte, but her account had not been hacked. Rather, scammers had used her name and Facebook profile picture to front a new Instagram account, then messaged all her Facebook friends via the Messenger service. The messages began with a simple 'Hello. How are you doing?' When her contacts replied, the fake Bronte sent a chatty response, explaining that 'she' had just undergone eardrum surgery and so couldn't have phone calls, before chattily asking how the recipient's family is. 'Bronte' went on to talk about a $50,000 grant she had received, sharing a link so that the real Bronte's friend could apply, too. Bronte's friend refused to click the link unless the 'Bronte' she was communicating with would take a call. They refused, citing the 'eardrum surgery', and so it was at this point Bronte's friend messaged the real Bronte another way, uncovering that it was all a scam. It is hard to know what clicking the link in the phishing messages would have done, for example it could have infected Bronte's friend's device with malware, or it may have sent her to a website aimed to deceive her into sharing personal and financial information.

Impersonation scams, much like the criminals operating them, take many guises. In recent years, some criminals

have exploited the authority, trust and adoration associated with celebrities by using their images to fraudulently front their scams. These cases include romance fraud, appeals for fraudulent charities, fraudulent endorsements of products and investment scams.

Sat on his sofa in Cologne, Germany, 42-year-old Sebastian was scrolling Twitter after his wife had gone to bed. He saw a tweet from Elon Musk, simply saying 'Dojo 4 Doge' and, below, it seemed that Musk had added replies with a link to a slick website where Musk's Tesla team appeared to be giving away Bitcoin. A competition, complete with countdown clock, was offering to double the Bitcoin that 'winners' sent. Sebastian sent 10 Bitcoin (at the time worth over half-a-million dollars) and waited for double the amount of funds to be returned into his Bitcoin wallet. When the cryptocurrency failed to appear, Sebastian realized he had been tricked:

> 'I'd just thrown away the gamechanger for my family, my early retirement fund and all the upcoming holidays with my kids.'[6]

Although the real Elon Musk had tweeted 'Dojo 4 Doge', the replies were impersonators, using his profile picture and with a screen name that looked very similar to his.

As the richest person in the world, an extroverted risk-taker and vocal fan of cryptocurrency, hijacking Elon Musk's image is an attractive ploy for social media scammers. As Chapter 12 explores, investment scams are prolific. In the first half of 2021 alone, fraudsters stole at least $2 million from cryptocurrency investors who were manipulated by fake Elon Musk scams.[7] Most of the scams

which impersonate Musk on social media pose as him promising giveaways of cryptocurrency – the criminals convince victims to invest a sum of cryptocurrency with a promise from 'Musk' that much more will be returned to them. Other scams involve a fake launch of a cryptocurrency supposedly backed by Musk or Tesla, pushing people to invest (Musk has said that neither he nor any of his companies will create a new crypto token). In 2023, multiple deepfake videos of Elon Musk (and news and television personalities) flooded social media platforms including Facebook, YouTube and TikTok. The videos, many of which were published on hacked YouTube channels with large numbers of subscribers, falsely claimed that Musk had launched a new investment platform, pushing viewers to fraudulent investment schemes.

The popular YouTube channel Linus Tech Tips was one of many that were hacked and used in Elon Musk impersonation scams. In March 2023, criminals sent what appeared to be a PDF to an employee on the Linus Media Group team. The document was malicious and, when it was opened, malware infected the device, able to steal user data from the browser. The criminals used this to bypass passwords and 2FA, taking over the Linus Tech Tips YouTube channel and broadcasting a cryptocurrency scam fraudulently using Musk's image to over 15 million subscribers.[8]

Taking the Elon Musk cryptocurrency scams a step further, a deepfake video of the popular British consumer finance expert Martin Lewis was shared in 2023 on Facebook adverts. The deepfake video made it appear as if the trusted TV figure was endorsing a 'new product' from

Elon Musk which 'opens up great investment opportunities for British citizens'. Lewis is widely regarded as the most trusted man in Britain, with those over 50 years of age trusting him more than any other source of financial advice, including their friends, their own research, financial advisers and banks.[9] In 2018, Lewis launched a lawsuit against Facebook after discovering that his image was being used to front fraudulent adverts on the platform, most of which were pushing cryptocurrency schemes. He felt that Facebook was not doing enough to control scam adverts such as these but dropped the lawsuit when the social media platform agreed to donate £3 million to set up an anti-scam project and take more action against scam ads on their site[10] When the deepfake scam emerged in the summer of 2023, a BBC interview with Lewis about the social media deepfake scam showed how furious he was about it. He said he felt 'sick' and that:

> 'These people are trying to pervert and destroy my reputation in order to steal money off vulnerable people. And frankly it is disgraceful, and people are going to lose money and people's mental health is going to be affected. It has a massive impact on well-being when people are scammed, it's devastating for people's lives, and we still don't have any adequate regulation to deal with it.'[11]

Celebrities feel familiar to us, we often relate to them and respect them, aspiring to be more like them. It is also common to bestow a sense of authority on celebrities, trusting their judgement. They are seen as successful, with a high status. Celebrity social proof is therefore valuable: when a public figure is seen to endorse a product, it affords

that product legitimacy and desirability. Celebrity endorsement scams exploit this sphere of influence, costing victims money and mental anguish along the way.

Some celebrities face scrutiny for their endorsements. After the collapse of the cryptocurrency exchange platform FTX, celebrities who endorsed it are facing lawsuits for lending credibility to the failed cryptocurrency exchange. Eleven celebrities including Tom Brady (former NFL quarterback) and Gisele Bündchen (one of the highest paid models in the world) were FTX ambassadors and advisers, with Brady paid $30 million (largely in stock) to promote the exchange in TV commercials as 'the most trusted' institution in cryptocurrency. Now a group of FTX customers are suing the celebrities, seeking compensation.[12]

Fake goods

Fraudulent giveaways are an increasing – and increasingly lucrative – social media scam for cyber criminals. In the first three months of 2021 alone, cyber criminals defrauded over $18 million from victims with these schemes.[13]

As well as pretending to give away cryptocurrency, goods or gifts, cyber criminals also impersonate, and fabricate, brands with a scam that involves the sales of goods that simply do not exist. The number of people being victimized by this particular strand of social media scam continues to grow, with it making up the most frequently reported fraud loss to the FTC in the first half of 2023.

These scams generally begin with adverts on Facebook or Instagram and most reports to the FTC were for clothing and electronic device purchases that never materialized.[14]

Alongside fake goods that never existed in the first place, criminals also use social media to sell counterfeit goods. Much like the scams above which impersonate individuals, social media adverts are used so prevalently in this that the FTC has asked the platforms to explain the steps they take to manage this problem.[15]

Research from Portsmouth University found that counterfeiters are piggybacking on the popularity of influencers to sell counterfeit products, which can be harmful to consumers and to the people working in unsafe counterfeit factories for low wages. The research suggests that as many as one-fifth of UK consumers who are active on social media have bought counterfeits endorsed by influencers, with teenagers three times as likely to do so and teenage boys accounting for 70 per cent.[16]

Fake influencer opportunities

It is, unfortunately, not surprising that fraudsters exploit the 'influencer economy'. Cyber criminals follow the money, focusing on platforms and trends that experience high growth with opportunities that they can exploit: in 2023, the influencer marketing economy was valued at $21.2 billion, and it has more than doubled since 2019.[17] Criminals use social media to exploit the rise of influencer marketing in various ways, especially with brand-ambassador scams. Posing as an established brand, the fraudsters

will 'recruit' people on social media with the promise of being an ambassador or influencer for them.

I spoke with Alastair Gray, who has 17 years working in investigations and a focus on anti-counterfeiting and online brand protection, about the biggest scams that he encounters:

> 'From my experience within the fashion industry, the most common scams are "brand-enabled" or "brand-weaponized" scams, whereby the name or logo of a popular fashion company is used in fake influencer recruitment accounts. These accounts would suddenly appear and request to be "followed" and shared with five friends by their victims in order to quickly boost their own engagement levels. I see these scams linking to off-platform websites or forms where users would be asked to provide account information including passwords in order for the criminals to get control of their accounts on the basis of "verifying" the victim's suitability as an influencer. The most concerning incidents relating to these types of accounts would be when they specifically targeted children and would engage in private messaging chats to try and receive commission fees or even photographs from the victims, again to determine their "influencer" credentials.'

As Gray highlights, criminals carrying out these scams use the lure of a promise to become an influencer with the aim of stealing personal or financial information, taking over the accounts or even convincing the victim to share photographs, which can escalate into image-based sexual abuse (see Chapter 4). By impersonating well-known, trusted and aspirational brands, some of these scams target

established influencers in a version of CEO fraud that has evolved over into social media, convincing influencers who may already be linked with a brand to make payments or share personal information which can then be used in identity fraud:

> 'A common influencer-related scam that appeared in 2022–23 appears to target people who have a social media presence and engaged with the official brand account, but the approach arrives by a free (but brand-related) email address. The scammers come complete with two-to-three-page "Social Media Influencer" contracts to be signed (with the actual CEO's name and a made-up signature already countersigned) and who are replying to interactions quickly (and demand a sense of urgency) stating the opportunity will quickly close. Once they get the victim interested, they ask the intended victim to cover the "shipping fees" for 10 items of clothing that the victim selects from the official brand website. This interplay between the real website and the brand-related email address adds to the legitimacy. When the shipping payment request is made there are a variety of options from PayPal Friends and Family accounts (just an email address) or gaming gift cards, but even Apple Pay, and it's usually a low amount under 100$ /100€. At the same time the victim gets an email from a "shipping manager" who asks to confirm other personal information to send out the package and these come branded as well including FedEx, UPS and US Postal Service. As quickly as the email addresses were shut down, new ones were quickly registered, and the scam continued.'

Fake jobs

Fake influencer opportunities are not the only recruitment scams on social media.

Adam saw a job advert on Facebook, offering the chance to 'extend your earning capability with minimum effort input', working flexible hours online from home adding 'you were never a supporting role!'.[18] When he applied and was contacted on WhatsApp to be offered the job, he was told the opportunity was with the company that handled the e-commerce for the luxury Italian retailer Luisaviaroma. Adam was given a demonstration of the company's platform and told that in his role as buyer, he would buy products which someone else would sell, leaving him with a large commission. The website looked legitimate, with logos and copywriting that was on brand, so Adam got to work but after five days – and having transferred $28,000 AUD (equivalent to $18,000) – he realized it was a scam. Adam's losses were among $9.6 million AUD defrauded from Australian victims in 2022, with most of these job recruitment scams beginning on social media, followed by messaging platforms such as WhatsApp.[19]

In the UK, Theo also found himself the victim of a recruitment scam.[20] Having been job hunting for a year, he was homeless, relying on insecure temporary income and sleeping on friends' sofas; he was desperate when a new opportunity came his way. Hired for a new role, his employer first told him he had to pay £275 for an HR qualification. With the promise of a regular income, he complied and started his first day. Theo was then told he would be in a

recruitment role and to fulfil the role, he needed a burner phone and to pay the subscription for a job-hunting site. He started making calls, speaking to people who were just like him before this opportunity, desperate to find work. After three days, he accepted that it was a pyramid scheme, realizing that the script he had been using to interview people was the same script that had been used on him.

Theo's experience is a reminder that – sometimes – it is not only the direct victims being exploited in these scams. It is as easy to think that all of those committing cyber crime are heartless, as it is difficult to wonder how they sleep at night. There are certainly many scams committed knowingly and ruthlessly. But the reality is also more complicated, with the deeply shocking and disturbing truth of how some of these scam operations run. In August 2023, the United Nations published a report about the 200,000 people that they estimate are being forced by criminal gangs to commit cyber crime in Southeast Asia scam centres.[21] The UN explain the two sets of victims here: those who are defrauded in scam operations and those who are coerced into working for some of the same operations, enduring abusive and inhumane treatment. Most of these victims of trafficking are not citizens of the countries where they are held, having moved there with a fraudulent promise of legitimate work.

Social media scams are widely used in the scam operations that abuse so-called 'cyber slaves':

> 'The prominent role of social media and other digital platforms is an inherent – and striking – feature of these online scam operations.'[22]

Ali and his cousin Ahmad were seeking jobs abroad to enable them to escape the economic hardship in Pakistan that had been caused by massive flooding. Ali borrowed $4,000 from family and friends to pay an agent for a tourist visa that would enable him to reach Cambodia, where he and Ahmad were met by a broker. They paid the broker a further $1,475 each for a work visa processing fee, before being taken to a large compound in Cambodia's capital, Phnom Penh. After their passports were taken and they were warned not to try to leave, they were forced to work alongside approximately 1,000 other people, each forced to scam five people daily with cryptocurrency investment schemes. They were watched over, fined and beaten if they failed to comply:

> 'I felt helpless taking away money from other people. There were many nights I couldn't sleep well because of the guilt, but I had no other choice.'[23]

After five months, Ali and six others were able to escape with the help of the Cambodia police. The operation, apparently run by an organized Chinese criminal gang, moved out of the building shortly after the rescue.

Fake news

Misinformation and disinformation are a serious problem for social media sites. While social media and other connected technology helped many of us navigate the Covid-19 lockdowns, it also contributed to a wave of

misinformation and disinformation that exploited the pandemic.

One false claim that spread on social media platforms was that 5G mobile phone signals transmit the virus or reduce our defences to it, despite scientists robustly debunking the theories. Videos were shared on social media showing mobile phone masts set on fire. Over the Easter weekend in the UK, there were 20 reports from mobile phone companies in the UK that phone masts were attacked, including one mast which served Birmingham's Nightingale hospital.[24] In Bolivia, where there was no 5G technology, the claims swirling around social media still prompted people to attack antennas.[25]

While 'fake news' has been around since ancient times, the growth of social media has enabled misinformation and disinformation to grow to a whole new level. As social media sites are structured to 'reward' people who share more content (with engagement metrics such as followers, views, reposts and likes), people are encouraged to share information more than they are encouraged to fact-check it. As Professor Wendy Wood, a psychologist at USC, has said:

> '[Misinformation is] really a function of the structure of social media sites themselves.'[26]

While we can focus on the spread and impact of disinformation, there is another question to consider: where does it come from? The answer suggests that most disinformation comes from a small number of sources. Research from the Center for Countering Digital Hate (CCDH) explored disinformation being spread about the Covid-19 vaccine.

Analysing anti-vaccine content that was shared or posted on Facebook and Twitter 812,000 times over the course of 6 weeks in 2021, the CCDH found that a staggering 65 percent could be linked back to just 12 individuals.[27] The so-called 'Disinformation Dozen' that the CCDH refer to are alternative health gurus, politicians, physicians and chiropractors, with a combined following of over 59 million people. While social media platforms have promised to increase controls to restrict and remove disinformation, the CCDH research claims that 93 per cent of reported posts were not removed and that, since the publication of the CCDH report, only three of the 'Disinformation Dozen' have been removed from just one platform.

Surging social media scams

In this chapter, I have explored just some of the ways that cyber criminals use social media to defraud us. These scams have grown hugely in recent years and show no signs of slowing down. According to data from the US Federal Trade Commission, one in four people who reported losing money to fraud since 2021 said it started on social media, with reported losses to social media scams hitting $2.7 billion that year.[28]

Scams can affect all social media users. The personal nature of social media provides profitable breeding ground for criminal schemes, enabling fraudsters to impersonate or create trusted personas, compromise accounts and even abuse legitimate advertising tools to target people. Criminals are drawn to social media for many of the same

reasons the rest of us are – it's a way to connect with people all over the world, scaling up and expanding interactions. Unfortunately, social media enables criminals to paint a veneer of legitimacy on themselves, as Gray commented:

> '[The proliferation of scams on social media] comes down to persistence of the scammers even after having multiple accounts shut down, but also the ease of setting up an account and the challenges as a user to verify whether the account is legitimate or not since any account can put the brand URL in the bio. Also, platforms lend themselves to sharing information, personal interests and photos so for scammers it can prove a rich seam of potential victims.'

More money was lost to fraud over social media than any other communication method: compared to the $2.7 billion reported losses for these scams, fraud over websites and apps cost victims $2 billion, phone calls $1.9 billion, email $0.9 billion and texts $0.4 billion.[29]

As the cases in this chapter will show, people of all ages can be scammed on social media. However, most likely due to more use of the platforms, younger people are more vulnerable to fraud over social media platforms. For victims of fraud aged 18–19 years, FTC analysis found that social media was the contact method of the fraudsters in almost half of all cases, 47 per cent. For victims aged 19–20 years, it was the contact method in 38 per cent of cases and the number continues to decrease with age.[30] This reflects research from Lloyds Bank, which found that those aged 18–24 years are most likely to become the victim of investment scams spread on social media, closely followed by those aged 25–34 years.[31]

These findings remind us that we can all be vulnerable to social engineering and scams, even 'digital natives' who are often regarded as more savvy with technology than those of us who grew up without the internet. The right phish – or fraud – at the wrong time can catch any of us. This is why we all need to be aware of how criminals use technology to manipulate and attack us, and what we can do to enjoy the benefits of that technology while staying safe from harm.

Stay social media savvy

Social media offers endless opportunities for us to connect, share, learn, network and build communities. It can be a great place for brands and businesses to grow and for all of us to see the world from different perspectives. Cyber criminals also, unfortunately, use social media to grow, connecting with and exploiting the rest of us. Scammers will always follow the numbers and the money. When a platform grows, criminals will be finding ways to exploit the increasing number of people using it – and unfortunately, there are many more scams than those which I have been able to cover in this chapter exploring the most common issues.[32]

With Gray's experience investigating counterfeiting and protecting brands online, he recommends verifying communications are legitimate, being alert to signs of scams and protecting our information:

> 'Brand-enabled scams are challenging as they could well seem legitimate, especially if the social media user has not interacted in the "corporate world" of contracts and agencies and is not familiar with how talent recruitment works in reality. It's easy to trust accounts that use words like "official" or "HQ" and try to operate as if they are a marketing team working outside the usual channels. The key advice would be that if you are a fan of the brand, you probably know their main account and it's okay to ask them to confirm if an approach is real either via their social accounts or better still via their official website. Look out for accounts that have few posts – that could be a warning sign of a scam and never give out login credentials. Ever!'

General good security practice on social media and messaging apps include:

1. Protect your social media accounts to keep them safe from account takeover, which not only protects your information and use of the sites, but also helps your connections stay safe – if your account is compromised, it could be used to phish your friends, family and colleagues. Using strong, unique passwords in combination with two-factor authentication is vital, which I explored in more detail in Chapter 2.
2. Be wary of social engineering, which cyber criminals are increasingly carrying out over social media, using tactics covered in Chapter 1.
3. If you receive messages from family members (or anyone!) asking for money, always verify these are legitimate by checking with the supposed sender by another communication channel.

4 Although many large and small businesses use social media adverts legitimately, criminals also abuse them. While we wait for the social media platforms to clamp down on scams being spread over legitimate adverts, it is important not to implicitly trust the adverts we see on social media. Before you buy, spend a little time researching the company, for example by searching online for its name plus 'scam' or 'fraud'.
5 Review the privacy settings of your social media accounts to make sure that you are sharing information in a way (and with others) that you are comfortable with, blocking and reporting suspicious accounts and content to help the platforms identify scammers.
6 Be mindful of misinformation and disinformation on social media, engaging critical thinking and checking facts before reposting or supporting content, especially if it is emotive and potentially divisive.

When it comes to avoiding cryptocurrency investment scams:

1 Ignore promises of free money or guarantees of high returns, and be wary of anything that uses a sense of urgency and time pressure.
2 Research any cryptocurrency platform or digital wallet provider before you share any data or transfer funds.
3 Don't invest in cryptocurrency schemes that are recommended by someone you have only communicated with online, even if you believe you have built up a friendship or relationship.
4 Never share your private keys (the codes that protect access to your virtual currency) and store them securely.

To stay safe from job recruitment scams:

1 Use reputable job-hunting sites rather than social media and messaging apps.
2 Avoid jobs where you are told to pay a fee or purchase items with your own money.
3 Be wary of opportunities with vague details that promise high salaries.
4 Tell people you trust about possible opportunities and sense-check anything suspicious with them.

And before I end this chapter, I must share one more story as a reminder that social media can sometimes help us in the fight against criminals. In March 2021, Marc Feren Claude Biart was living a quiet life in the Dominican Republic when he decided to start a YouTube channel about Italian cooking. He didn't show his face, but the reported mafia fugitive did show his arms with distinctive tattoos. Biart was an alleged member of the 'Ndrangheta crime syndicate, said to be Italy's richest and most powerful crime organization. Having been on the run from Italian police since 2014, those YouTube clips of his tattoos enabled police to track his movements, finding and arresting him in the Dominican Republic.[33] This isn't the first time a criminal has been undone by their eagerness to overshare on socials, and it won't be the last.

Notes

1 Clark, J and Hern, A (2023) 'I felt stupid and embarrassed': victim of 'Hi Mum' fraud on Whatsapp lost £1600, *The Guardian*, 16 June. www.theguardian.com/technology/2023/jun/16/victim-of-hi-mum-on-whatsapp-lost-1600 (archived at https://perma.cc/UUF8-25W9)

2 www.9news.com.au/national/scammer-fleeces-42000-from-adelaide-father-through-online-messaging-platform/95acfc36-b245-4d88-9d22-22babc8f7cb1 (archived at https://perma.cc/PH4V-BUU9)
3 www.which.co.uk/news/article/notorious-hi-mum-and-dad-scam-spreads-from-whatsapp-to-text-message-an7N34c0gVbP (archived at https://perma.cc/7DAK-PYCS)
4 www.theguardian.com/money/2023/feb/20/cruel-scam-of-mum-and-dad-sparks-a-regulatory-crackdown (archived at https://perma.cc/D2A7-HFH4)
5 Gossling, B (2022) 'A scammer impersonated me and tried to fleece my friends, but Instagram said it didn't violate Community Guidelines', 9 Honey. honey.nine.com.au/latest/instagram-phishing-scam-impersonator-accounts-do-not-violate-community-guidelines/30473250-2a18-45ca-9145-9360c4dec6bd (archived at https://perma.cc/S3HJ-VB3M)
6 Tidy, J (2021) Bitcoin: Fake Elon Musk giveaway scam 'cost man £400,000', BBC News, 16 March. www.bbc.com/news/technology-56402378 (archived at https://perma.cc/WE8C-BDNQ)
7 Iacurci, G (2021) Elon Musk impersonators stole more than $2 million in crypto scams, regulator says, CNBC, 17 May. www.cnbc.com/2021/05/17/elon-musk-impersonators-stole-more-than-2-million-in-crypto-scams-.html (archived at https://perma.cc/M3J4-GRYY)
8 Linus Tech Tips (2023) My channel was deleted last night. youtu.be/yGXaAWbzl5A?si=4_sYng9RwtgaaXUy (archived at https://perma.cc/6PZU-2GGR)
9 Russell, B (2023) Martin Lewis more trusted by 50-90-year-olds than financial advisors, IFA Magazine, 12 March. ifamagazine.com/martin-lewis-more-trusted-by-50-90-year-olds-than-financial-advisers/ (archived at https://perma.cc/D7SB-E8MQ)
10 Hern, A (2019) Martin Lewis drops lawsuit as Facebook backs scam ads scheme, The Guardian, 23 January. www.theguardian.com/technology/2019/jan/23/martin-lewis-drops-lawsuit-as-facebook-backs-scam-ads-scheme (archived at https://perma.cc/CMA9-3FFE)
11 BBC News (2023) Martin Lewis felt 'sick' seeing deepfake scam ad on Facebook, BBC News, 7 July. www.bbc.com/news/uk-66130785 (archived at https://perma.cc/2E4Y-QLDP)

12 Griffith, E and Yaffe-Bellany, D (2023) How Tom Brady's crypto ambitions collided with reality, The New York Times, 6 July. www.nytimes.com/2023/07/06/technology/tom-brady-crypto-ftx.html (archived at https://perma.cc/MR4U-FBCG)
13 Tidy, J (2021) Bitcoin: Fake Elon Musk giveaway scam 'cost man £400,000', BBC News, 16 March. www.bbc.com/news/technology-56402378 (archived at https://perma.cc/AKQ4-DCGA)
14 Fletcher, E (2023) Social media: a golden goose for scammers, Federal Trade Commission, 6 October. www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers (archived at https://perma.cc/935P-XUVL)
15 Fair, L (2023) Bad ads on social media: FTC asks platforms about their screening policies, Federal Trade Commission, 22 March. www.ftc.gov/business-guidance/blog/2023/03/bad-ads-social-media-ftc-asks-platforms-about-their-screening-policies (archived at https://perma.cc/3AKR-S3U4)
16 Macaulay, T (2023) Influencers have made social media booming market for counterfeit goods, study finds, The Next Web, 10 August. thenextweb.com/news/social-media-influencers-selling-counterfeit-goods (archived at https://perma.cc/ET55-TCPT)
17 McKinsey & Company (2023) What is influencer marketing? McKinsey & Company, 10 April. www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-influencer-marketing (archived at https://perma.cc/EV2Y-GQEL)
18 Silva, A (2023) Adam thought he was starting a new job, until he lost $28,000. What are recruitment scams and how are they targeting job seekers? ABC News, 29 January. www.abc.net.au/news/2023-01-30/what-are-recruitment-scams-targeting-job-seekers-australia/101875596 (archived at https://perma.cc/RPH5-B9R5)
19 NACS Scamwatch (2023) The most devastating employment scams in 2022 happened via social media, with victims told they could earn several hundred dollars for little effort while working from home, 20 April. x.com/Scamwatch_gov/status/1649231507783909382?s=20 (archived at https://perma.cc/TU9Q-29F4)
20 Franks, J (2023) Scammed out of money and tricked into fake work – the recruitment cons costing jobseekers thousands, Sky News, 2

April. news.sky.com/story/scammed-out-of-money-and-tricked-into-fake-work-the-recruitment-cons-costing-jobseekers-thousands-12822185 (archived at https://perma.cc/3JRQ-25BZ)
21 Office of the High Commissioner for Human Rights (2023) Hundreds of thousands trafficked to work as online scammers in SE Asia, says UN report, United Nations Human Rights, 29 August. www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report (archived at https://perma.cc/BBG8-CF6B)
22 Office of the High Commissioner for Human Rights (2023) Hundreds of thousands trafficked to work as online scammers in SE Asia, says UN report, United Nations Human Rights, 29 August. www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report (archived at https://perma.cc/B8AJ-MAGG)
23 IJM. Survivor of cyber slavery: 'I was sold and forced to scam people'. ijmhk.org/en/survivor-of-cyber-slavery-i-was-sold-and-forced-to-scam-people/ (archived at https://perma.cc/B8AJ-zzzz)
24 Kelion, L (2020) Coronavirus: 20 suspected phone mast attacks over Easter, BBC News, 14 April. www.bbc.com/news/technology-52281315 (archived at https://perma.cc/UN3E-K6YH)
25 Goodman, J and Carmichael, F (2020) Coronavirus: 5G and microchip conspiracies around the world, BBC News, 27 June. www.bbc.com/news/53191523 (archived at https://perma.cc/5SK6-93CR)
26 Madrid, P (2023) USC study reveals the key reason why fake news spreads on social media, USC Today, 17 January. today.usc.edu/usc-study-reveals-the-key-reason-why-fake-news-spreads-on-social-media/ (archived at https://perma.cc/YNL8-JMT2)
27 Center for Countering Digital Hate (2021) The disinformation dozen. s3.documentcloud.org/documents/21011322/disinfo-dozen.pdf (archived at https://perma.cc/GPW2-RUC6)
28 Fletcher, E (2023) Social media: a golden goose for scammers, Federal Trade Commission, 6 October. www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers (archived at https://perma.cc/9YMA-9B7C)
29 Ibid

30 Ibid
31 Ziegler, L (2022) Insta-scam: how scammers are targeting younger users online, Lloyds Banking Group, 5 May. www.lloydsbankinggroup.com/insights/how-scammers-are-targeting-younger-users-online.html (archived at https://perma.cc/KLE5-F42Q)
32 Barker, J (2022) How to avoid the most common WhatsApp scams. youtu.be/6xejzya19yE?si=4txOJh3k1QaJes6g (archived at https://perma.cc/2WCC-ZWLJ)
33 Giuffrida, A (2021) Mafia fugitive caught after posting YouTube cooking video, The Guardian, 29 March. www.theguardian.com/world/2021/mar/29/mafia-marc-feren-claude-biart-caught-youtube-cooking-video (archived at https://perma.cc/64ZM-92SM)

CHAPTER EIGHT

Malicious insiders

When a cyber security incident or data breach involves somebody inside an organization, it is generally not malicious. Most 'insider' incidents happen when someone makes an honest mistake. The root cause can most often be found in the context and system: someone being overworked, distracted and under pressure, by a lack of training, inadequate tools, training and guidance, or by too much friction in processes and procedures. It can be a combination of all of the above.

Occasionally, insider security incidents occur by design. Malicious insiders are rare, but when someone within an organization chooses to disrupt or defraud that organization, it is often extremely damaging and costly. If someone within an organization wants to steal information or cause

havoc, they are well-placed to know how to do it and are more able to use their position from within, to go undetected.

What motivates malicious insiders?

In some cases, malicious insiders join an organization with the intention of abusing their position. They may work for an organized criminal gang or be working on behalf of another government, or they may be an activist with an ideological cause against the company. However, most malicious insiders do not start out with the intent to attack their organization.

Malicious insiders are most commonly loyal employees before they turn against their employer. They often develop a grudge against the organization; for example, if they have been refused promotion or reprimanded in a way that they see as unfair. Malicious insiders often feel an external pressure; for example, with financial debts or changes in their personal circumstances, such as the break-down of a relationship. They can convince themselves that in stealing from or disrupting their organization, they are not engaging in criminal activity but rather righting a perceived wrong against them.

Other malicious insiders are led by ambition and opportunism.

In May 2023, a former IT security analyst was sentenced to jail for exploiting an external ransomware attack – and his position working for the victim company – to attempt to profit from the incident himself. Ashley Liles worked for

the gene and cell therapy company, Oxford Biomedica, when its systems were infected with ransomware in February 2018. A board member for the company reportedly received a blackmail email from criminals demanding $370,000. In his role as an IT security analyst, Liles was tasked with working alongside colleagues and law enforcement to investigate the attack and try to limit its damage.

Instead, Liles is said to have used his position to access the private emails of the Oxford Biomedica board member 320 times, at one point changing the ransom note sent from the criminals who had perpetrated the attack. He altered the Bitcoin payment address in the ransom note to one which belonged to him, with the hope that any payment made would therefore go to him. Liles then took this a step further, setting up an email address almost identical to the one being used by the criminals and sending emails pressuring Oxford Biomedica into paying the ransom.

Like many malicious insiders who are caught, Liles did not sufficiently cover his tracks. His unauthorized access to the board member's private emails was identified and police traced the access back to Liles' home. Forensic experts examined computers seized from his home and, despite Liles' attempts to wipe them, were able to recover evidence. After initially denying involvement in the crimes, Liles pleaded guilty to two charges before his trial began. He was sentenced to three years and seven months in prison for blackmail and unauthorized modification of computer material.[1]

At the time of sentencing, Judge Khan commented on the stress and anxiety that Liles had caused to the people

with whom he had previously worked. The judge referred to a statement from the CEO in which he said the consequences of Liles' actions had caused reputational damage and outside costs of £245,000.

From what we know of this case, it seems that Liles found himself in a position where temptation overshadowed any kind of ethics or conscience. His lawyer offered a defence that his actions reflected the immaturity of his age at the time of the offences, when he was 22 years old. We do not know if he had any other, misguided means of justifying his actions to himself. But we do know that many malicious insiders find a way of reconciling their behaviour to assuage any conscience they may have.

Formula 1 spygate

This certainly seems to have been the case with the 2007 Formula 1 (F1) incident that became famous as 'spygate', one of the biggest scandals to hit F1.

For the malicious insider at the centre of spygate, it appears that disgruntlement was at the heart of his actions. Nigel Stepney had a long career in motor racing, beginning as an apprentice aged 17.[2] He rose through the ranks and was chief mechanic at Ferrari when Schumacher ruled the racecourse in the early 2000s. He was recognized as playing a pivotal role in the team's success:

> 'He was widely credited for his diligent approach that gave Ferrari a reliability record that was the envy of the pit lane.'[3]

For his role in the success, Stepney expected a promotion – and was apparently sorely disappointed when he did not feel he received the recognition he was due.

Stepney responded by stealing 780 pages of confidential information, which served as the blueprints for the 2007 Ferrari F1 car. It's hard to think of more valuable, commercially sensitive information for the Ferrari F1 team. He then handed this paperwork to Mike Coughlan, chief designer at McLaren, with a view that they would both use the information as a springboard to secure new jobs at another team. The Honda Racing F1 team later released a statement acknowledging that Stepney and Coughlan approached them in 2007 to explore job opportunities.

Events did not go to plan for Coughlan and Stepney. Instead, their actions led to McLaren being fined an unprecedented $100m and being banned from the constructors' championship (the competition for the F1 team that secures the most points) that year.[4] Stepney was sentenced to 20 months in prison for sabotage, industrial espionage and sporting fraud and, although he did not serve the sentence, he never worked in Formula 1 again. But it is the details of how Coughlan and Stepney came undone which are the most bizarre and which remind us of the truly human nature of this topic.

Coughlin was seemingly not satisfied with the almost 800 pages of confidential information stolen from Ferrari and felt the need for a second copy. To achieve this, he handed the paperwork to his wife who took it all to a photocopy shop in Woking, England, and ordered a copy. Mrs Coughlin didn't realize that, when she handed over this stolen, secret information to the photocopy shop

owner, she was handing it to a Ferrari fan who was so suspicious that he would email Ferrari and cause the whole scandal to unravel.

In May of 2022, I had the good fortune to meet Mark Gallagher, a Formula 1 motor racing executive and author of *The Business of Winning*. We met at an event for technology leaders, where we were both speaking, and Mark not only delivered a captivating speech to a packed room, but he was also generous enough to spend some time chatting with me in the green room. We had a brief conversation about spygate and so, in writing this book, I knew I had to hear more of his thoughts and experiences:

> 'If it wasn't for this farcical situation where an employee of a photocopier shop in England spots that they have the IP of Ferrari in their shop! And the fact that the person in the copier shop just emailed the Ferrari website! We all think those contact forms on websites never get read by anybody and they get thousands of emails a day asking for autographs and so on – and yet they picked up on this message and unlocked the whole thing.
>
> Every team would know it won't be the last example of a disgruntled employee or just someone trying it on because they want to get a new job, so they decide, actually, they're going to take some of the company's data.'

The existence of malicious insiders is an uncomfortable truth for many organizations. It is unpleasant to think that people we work alongside and trust can turn on us or be plotting behind our backs. It can be easier to accept the idea of a faceless attacker in another part of the world, but

those inside the 'castle walls' can do more damage – from an information, financial and reputational perspective.

Malicious insiders are challenging from a psychological, operational and cultural perspective, which Gallagher addressed in our conversation:

> 'What I speak about to companies all the time is this whole approach to building a high performing team and, of course, when you talk about the values and behaviours of high performing teams – by which I mean the competitive F1 teams – they have incredibly successful leadership teams and have built a really strong culture. And embedded in the culture in high performing successful teams is a high degree of trust, a huge amount of respect, psychological safety (people are encouraged to speak out, you will be listened to, every employee is encouraged to lean into the job and deliver) and so you're trying to create this incredibly open, transparent culture where people share – share information, share knowledge, move information quite freely around the company – because one of the attributes of successful teams in F1 is the imperative of making sure the organization is on the same page and moving at the same speed.
>
> So we're trying to get a fully aligned, cohesive organization. A big group of people. In the case of Red Bull Racing today, there are 1,600 full-time employees, the Mercedes Benz F1 team is 1,800 employees. So these are not small sports teams, these are quite large technology businesses and we're trying to have strong cross-functional communication, and this is about trust and respect and safety.
>
> But the other aspect, the flip side of this is the recognition that the human condition means that not everyone will be

happy all of the time, that people move jobs, that we can't offer career development for everyone at the speed they want to go in. Staff retention is a really big focus, but you can't promote all of the people all of the time, so sooner or later you're going to lose people and we see a brain drain from the successful teams. You end up having to have this balance where, from a cultural perspective you want openness, honesty, transparency, psychological safety – really positive human values in terms of how you work together as a team – counterbalanced by the fact that the data being shared by people has to be treated as if you literally were putting money in their hands. If you imagine the data everyone has as bags of currency, you literally don't want them to leave the company with that.

There is an understanding that having robust policies around cyber security and data protection and the reason for that is very well understood. One of the benefits of spygate is that for an entire generation of people who worked in Formula 1, it became the reason why we had to do things the way we do them. So, when you get your laptop or mobile device or logon details and you go through the whole IT induction, they impress upon you the importance of data security, the way in which threats need to be avoided. Everyone gets it and spygate helped with that enormously.'

A wake-up call

Unless motivated by malicious purposes, no individual, organization or industry wants to experience a cyber security incident. They can be extremely costly, draining

(psychologically and emotionally, as well as financially), they can cause huge reputational damage and can threaten the continuation of a business and people's livelihoods. However, they can also influence positive change. Spygate was damaging, shocking and tragic. There were also positive benefits for the sector:

> 'It conclusively ended any debate, if there was any, within F1 leadership circles about the fact that our data, that data within an F1 team, was actually all of its value. The value of a team is its data, it's not the pounds and pennies in the bank account, it's that information. You see that manifest itself in 2023 in the fact that there isn't a single practice, qualifier or race that goes by without a driver or team principal talking about the data. It is the lifeblood of the sport. Spygate alerted people to the fact that we were in a decade of profound change. The years 2000 to 2010 was the decade when the sport grew up in terms of its use of data and we moved to not just gathering big data but actually analysing that. The advent of data analytics was really, primarily that decade. We really began to understand what we had in the palms of our hands, and this is why spygate came as such a shock, because it showed how easily information could be moved, how easily info could be copied. People were talking about cyber security; people thought the threats were all external – it turned out our biggest threat had been internal. So it changed the discourse around where the threats originate from. There was a lot of growing up done as regards spygate.
>
> At that point you would have had an IT director, and we were not very far past the point where the IT director sat in a little room at the end of the corridor, and you went

there to get your laptop fixed. It's ridiculous, but through the 1990s, IT was an office where stuff got fixed. Spygate really helped to accelerate the person responsible for information technology in a F1 team into the C-suite and, of course, nowadays no one thinks twice about the fact the CIO is not only a critically important role and person in the organization, but actually has moved from being operational into a strategic role. So there's been a really big shift and spygate played a role in that. There isn't a board of directors or management board in F1 today that isn't keenly aware of the importance of protecting data and spygate has become the pivot point for that, everyone knows the criticality of that. It was a game-changer for the industry.'

The impact of malicious insiders

The human impact of malicious insider cases should not be underestimated. Cyber security incidents often take their toll on those responding to and investigating them. For victims, there can be a psychological, reputational and financial impact. With malicious insiders, it can be the perpetrator who suffers the most from self-inflicted harm. In my conversation with Mark Gallagher, we explored this, and he shared insights from another case of a malicious insider:

'Benjamin Hoyle worked for me when I ran the Cosworth F1 engine company and Ben's forte was as a coder. He is one of these geniuses who can code an electronic control unit on any type of engine – racing, road car, rally car – he can write the program that drives the performance of that engine. Ben

> was one of the gurus. He went from us to Mercedes. The Mercedes Benz engine in Lewis Hamilton's car was one of the reasons for Lewis achieving world championship success, the engine was particularly innovative and high performing.
>
> So Hoyle was the guy who was coding the electronic control units for those engines – highly sought after. Sure enough he got an offer from Ferrari to come and work for them. He proceeded to download the data from Mercedes Benz onto three separate devices. The Mercedes Chief Information Officer had done their job properly and the systems immediately flagged that data had been accessed on an unauthorized basis. An investigation was carried out and they realized it was Ben, that he was going to work for Ferrari, and he was going to take Mercedes data with him, so they prosecuted him. Ferrari withdrew the job offer and Ben became instantly unemployable in F1. Here you have a really bright guy, central to Mercedes dominance as one of the key people within the team, and he decided he is going to outsmart Mercedes to try to arrive at Ferrari in a blaze of glory.'

In both cases, it appears that neither of those individuals had any real understanding of just what a serious crime they were committing.

Hoyle told Mercedes in 2014 that he would be leaving the organization in 2015 and it was expected that he would move to Ferrari. When Mercedes took legal action against Hoyle to 'protect its intellectual property', a Ferrari spokesperson said: 'It's not true he was on the verge of joining us. What he did concerns only him and the company he was working for. We are not involved in this.'[5]

There is another side to malicious insider cases, which is often overlooked. Companies and individuals can become paranoid about the threat, undermining relationships and organizational culture. The implication of malicious activity can also be weaponized. Gallagher and I discussed these elements:

> 'There is another twist to the tale. I know of someone very successful within F1 who was alleged to have stolen data when he moved teams. And he hadn't. In the end he took legal action against his former team and won, he secured damages. But the result of that entire process is that he had to leave the entire Formula 1 industry. He went from one very well-known team to another and the team he left was so upset, because he was a really key person, that the Chief Exec of the old team contacted the Chief Exec of the new team and said, "we think he's taken data with him and if we can prove it, we'll be coming after him". Because the allegation was made, the new team cancelled his contract. He couldn't understand why he had his offer of employment withdrawn. So, he eventually found out what had happened and he took the necessary legal action. So that gives another side into where this whole thing can go in terms of people making unfounded allegations, that can also be career-ending or limiting. In his case, because he was so well known, he had this cloud hanging over him and a general view there's no smoke without fire. So, he left the industry and set up his own company 10 years ago.
>
> [This reflects] a paranoia but also an interesting way of using this topic to damage people's reputations. It goes to show there are so many edges to this and it is not a simple topic.

> An allegation that you may have taken data with you is a little bit like the old allegation that someone had their hand in the till. The narrative is now there in the background that whenever people change teams that, somehow, they might be taking data with them.'

Malicious insiders and the human side of cyber security

Malicious insiders remind us that cyber security is a complicated subject, as much about human behaviour and motivation as it is about technology. These cases reinforce the importance of culture as much as they highlight the need for having the right policies and controls in place. In my experience, it can be challenging to communicate this to busy executives and business leaders, which Gallagher also reflected on:

> 'It's all too easy for people to think that because they have some systems in place, they are somehow covered. The reality, the sophistication of the threats is constantly evolving and therefore, in F1, just as we know that the way for us to prevent fatal accidents is to keep a constant, relentless, slightly wearisome vigilance around safety – it has to be relentless – it is the same with this topic.
>
> In talking to companies about technology and digital transformation, I very often encounter executives who will say "we're covered". Your advice has to be, we are on the edge of these threats all the time and that we just can't let up on our vigilance. It's not about fixing at a point in time,

it's about keeping constant vigilance and trying to stay one step ahead of the threats, and that is increasingly difficult in a complex, connected world. It's too easy for people to get to a point where they think they have it cracked because they have a few systems in place and actually, our experience is the threat is constantly evolving and changing, internally and externally.'

How businesses can protect against malicious insiders

Malicious insiders are rare, but often very damaging when they strike. If you are a business leader or owner, the following can help you mitigate the risk of malicious insiders:

1 Employee screening: malicious insiders are often loyal employees until they 'turn', so a clear background does not mean someone will never act maliciously, but in some cases malicious insiders have a pattern of criminal behaviour, therefore employee screening should always be conducted.
2 Least privilege: putting access controls in place based on the principle of least privilege means that employees only have access to data and systems that they need to carry out their role. Establish a process to regularly review and update access rights, alongside changing them when people move roles or leave the organization.
3 Network monitoring and data loss prevention (DLP): monitoring systems and using DLP solutions can help

you track activities, access and system changes; set up alerts alongside a process to regularly review the logs so that unusual activity can be identified.

4 Security assessments: penetration tests do not just look at how vulnerabilities can be exploited by external threat groups, but can also address internal vulnerabilities that could be exploited by a trusted party within the network.

5 Data encryption: encrypt sensitive data at rest and in transit to protect it from unauthorized access, even if an insider has access to it.

6 Security culture: a positive and proactive security culture can help mitigate malicious behaviour, because people will be more alert to unusual and suspicious activity.

7 Organizational culture: it can be a challenge to security leaders that wider organizational culture – factors beyond the control of security – are a factor in malicious security behaviour, but working with HR to understand changes to company structures and communications can help manage this issue.

Notes

1 Cluley, G (2023) Rogue IT security worker who impersonated ransomware gang is sentenced to jail, 12 July. grahamcluley.com/rogue-it-security-worker-who-impersonated-ransomware-gang-sentenced-to-jail/ (archived at https://perma.cc/G3AK-Y5YE)

2 Racefans (2023) Nigel Stepney, Racefans. www.racefans.net/f1-information/drivers/whos-who-s/nigel-stepney/ (archived at https://perma.cc/FJJ4-VER2)

3 Ibid

4 BBC Sport (2007) McLaren hit by constructors' ban, BBC Sport Motorsport, 13 September. news.bbc.co.uk/sport2/hi/motorsport/formula_one/6991147.stm (archived at https://perma.cc/7MSL-RMJ7)
5 Weaver, P (2015) Mercedes engineer Benjamin Hoyle at centre of spy row will not join Ferrari, The Guardian, 9 December. www.theguardian.com/sport/2015/dec/09/mercedes-ferrari-f1-benjamin-hoyle (archived at https://perma.cc/KGT6-C87Q)

CHAPTER NINE

Malware

It hasn't always been like this, but it is not hyperbolic to say that software runs the world. Useful software helps our washing machines run, our emails send, our lights go on, our institutions function and even allows our cars to drive themselves. It's helping me type this book and it's supporting my publisher in producing it. Maybe it's helping you read it. It is integral in our traffic lights, our aeroplanes, our microwaves and our phones.

That is not to say that software is perfect. Even software that is designed for good can go wrong, either by simply not working well or containing vulnerabilities or bugs that can be exploited by cyber criminals. The production of software – the software development lifecycle (SDLC) – often operates under tight time pressure. Companies generally feel the need to be first to market and so software

developers are often expected to produce results quickly, to quote Mark Zuckerberg's phrase (used as a Facebook internal motto until 2014) to 'move fast and break things'.[1] This inevitably can lead to errors in the code, meaning security flaws or bugs which are not spotted at the time of production, but which sometimes can lead data to leak or open up vulnerabilities for cyber criminals to exploit (see Chapter 3).

Beyond simply not being perfect, there is also a subset of software created to be actively malicious: to break or prevent services from being used, to infiltrate networks and obstruct operations, to exfiltrate data, to encrypt data, to disrupt and delay. Malicious software – malware – has been in existence for almost as long as the first daily use of computer systems.

The earliest forms of malware were relatively simple and often created for experimental or mischievous purposes. The Creeper program, created in the early 1970s, is considered one of the first instances of self-replicating code (also known as a worm). It spread across ARPANET, a precursor to the internet, displaying the message 'I'M THE CREEPER. CATCH ME IF YOU CAN!' While often regarded as the first computer virus, Creeper had no malicious intent and was actually designed to test security and see if a self-replicating program was possible.[2]

Worms

Worms are a subset of malware, they are a form of self-replicating malicious software designed to spread across

computer networks and systems, typically without requiring a human to interact with them once they are on the move. Self-replicating means that worms, unlike viruses, don't require a host file or application to spread. They can replicate themselves without attaching to other files or software, by exploiting vulnerabilities in the target system or by moving through the network, often piggybacking on legitimate functions. Worms spread through computer networks, exploiting vulnerabilities in network protocols or services, and they can use email, instant messaging and social media to distribute themselves. Most worms carry a payload, which is the part of the attack that actually does the damage. This payload can include activities like data theft, distributing additional malware, launching a distributed denial-of-service (DDoS) (see Chapter 11) or creating a backdoor to enable remote access by cyber criminals.

It's hard to remember (or – depending on your age – imagine) a time when we were not really aware of computer viruses, but in the 1990s, while many of us (myself included) might have been using computers to some extent and taking our first forays onto the World Wide Web, cyber (in)security was not hitting the headlines as it frequently does today.

Viruses

Then the Melissa virus came along, created by a programmer named David Lee Smith – and reportedly named after

a topless dancer in Florida. Smith had hijacked an AOL account and posted a file on a user group (a forerunner to internet forums) named 'alt.sex', promising free access to websites with adult content. However, when people downloaded and opened the Microsoft Word document which claimed to contain passwords to give the free access, they actually downloaded a virus. The Melissa virus worked by taking over the initial victims' Microsoft Word program, disabled features of the software to make it harder to detect the virus in action and then used a macro* to hijack their Microsoft Outlook emails, sending messages to the first 50 people in their mailing lists. Continuing the theme of the social engineering that began with the promise of free access to adult websites, these messages tempted recipients to open an attachment with names like 'sexxxy.jpg' and 'naked wife', attached to an email that read 'Here is the document you asked for… don't show anyone else;-)'. The recipients who opened the attachments didn't realize that, in doing so, they were infecting their computer with a virus.

The first reports of the Melissa virus were made on Friday 26 March 1999, and over the weekend, it had spread to over 100,000 computers at over 300 organizations. Although the virus was not intended to steal money or information, it still wreaked havoc and led to costs of approximately $80 million for the clean-up and repair of

*Macros are computer application tools that enable often-used commands to be automatically executed; macro viruses abuse the legitimate macro programming language to replicate themselves.

affected systems in the US alone. On a global scale, the Melissa virus is estimated to have cost $1.1 billion in recovery costs, affecting countries including Singapore, New Zealand, Sweden and Qatar.[3] Smith was quickly identified by authorities, with the assistance of AOL, and after being arrested in New Jersey, US, on 1 April 1999, was sentenced to 20 months in federal prison, fined $5,000 and agreed to cooperate with federal and state authorities.[4] It seems that Smith's motivation was one of curiosity and mischief: he simply wanted to see if his virus would work. One month later, in April 1999, testimony before the Subcommittee on Technology in the United States House of Representatives concluded that:

> 'Federal agencies were fortunate that the worst damage done by Melissa was to shut down email systems and temporarily disrupt operations… it is likely that the next virus will propagate faster, do more damage, and be more difficult to detect and to counter.'[5]

The Melissa virus gave the public and authorities a taste of the threat posed by cyber insecurity, waiting on the horizon. It encouraged greater focus on cyber crime and information security concerns across government and the private sector, highlighting not just how quickly viruses can spread but also bringing to light the limited countermeasures that were in place. As the FBI have since reflected:

> 'For the FBI and its colleagues, the virus was a warning sign of a major germinating threat and of the need to quickly ramp up its cyber capabilities and partnerships.'[6]

As the Subcommittee on Technology testimony acknowledged at the time, it demonstrated the importance of cyber security awareness and the extent to which people are a critical layer of defence, able to be a strong link in the security chain when empowered to do so:

> 'Melissa proved that computer users can do a good job of protecting their systems when they know the risks and dangers of computing and when they are alerted to attacks… organizations that trained their employees and warned them of attack fared much better than those that did not.'[7]

Unfortunately, the Melissa virus also inspired copycat viruses and can be seen as the start of the end of the internet's age of innocence.

Less than a year after Melissa, came ILOVEYOU – the next iteration of malware worms. With both viruses, a key theme emerges that has come to be one of the most misunderstood yet defining elements of cyber security: it's not just about technology, but equally about human psychology and behaviour.

The global reach of malware

In May 2000, about 50 million people around the world received a love letter in their inboxes: an email with the subject line 'I Love You' and an attachment LOVE-LETTER-FOR-YOU.TXT.vbs. Who could resist such a flattering, tempting proclamation, especially in the days when phishing emails were not as common – or known – as they are now? Once again, even in these early days of

the emergence of cyber insecurity, social engineering is front and centre.

Mikko Hyppönen is a technology speaker and author of *If It's Smart, It's Vulnerable*. He sits on numerous cyber security and technology boards, including serving as an Advisory Group Member at Europol. Since 1991, he has worked at the global cyber security and privacy company, F-Secure. The F-Secure research team was the first to find out about the ILOVEYOU virus, and I heard from Mikko first-hand about how it played out. He told me how Katrin Tocheva, an F-Secure anti-virus researcher, opened an alert email at 9.41 am in Finland, with a request for help from a US computer manufacturer with the ILOVEYOU virus attachment, routed to the team from another F-Secure office. Less than 30 minutes later, another one came in. One minute later, another followed. By 10.29 am, they had received five requests for help, from clients in the US, the Netherlands and South Africa. As the day unfolded, they received one sample of the virus every five minutes or less, coming from countries including the US, the Netherlands, South Africa, the UK, Finland, Estonia, Belgium, Norway and Italy. By 12.23 pm, the anti-virus team had received an email from F-Secure's London office reading, 'This is a big one guys. 600 copies in two hours.'

As Hyppönen reflected, it took six hours for Melissa to spread around the world, whereas ILOVEYOU took two hours. Melissa was limited in that the virus could only copy up to 50 addresses from your personal address book, but couldn't access business or corporate databases, yet ILOVEYOU latched on to every address that was

accessible through your Outlook on your machine. Looking back at it now, this is what Hyppönen had to say:

> 'ILOVEYOU was malware from a different, more innocent era. It might have been one of the largest outbreaks in history, but it was not done to make money, or to wage war or to breach our privacy. It was simply written to spread. There was no higher motive, no mystery, no drama. Malware outbreaks like these are now long gone.'

So, who was behind ILOVEYOU, why did they unleash it on the world and what happened to them? Police in the Philippines identified 23-year-old computer student Onel de Guzman as the man behind the malware, but no arrest or prosecution followed. The incident brought to light the fact that there were no laws in the Philippines against making malware, which was swiftly addressed by the creation of the E-Commerce Law a couple of months later. With the Philippines constitution banning the retroactive application of legal consequences, de Guzman was never prosecuted. Final analysis of the incident concluded that, within 10 days of ILOVEYOU (also known as the Love Bug) being unleashed, 10 per cent of internet-connected computers around the world were infected and the total financial damage was estimated to be approximately $10 billion.[8]

Twenty years later, after ILOVEYOU spread around the world, the investigative journalist and author Geoff White spent a year chasing leads to track down de Guzman, with the hope of finding out whether he really did create ILOVEYOU. In his book *Crime Dot Com*, White spoke

with de Guzman, reflecting on his role in the history of technology and cyber security. De Guzman told White that, as a poor student seeking expensive access to the internet, he had created ILOVEYOU with the aim of stealing other people's passwords and using the internet access they were paying for. He saw internet access as a human right and, as part of his university studies, had created a password-stealing program that took advantage of a flaw in Windows 95. He just needed to find a way to get people to click and, as he told White:

> 'I figured out that many people want a boyfriend, they want each other, they want love, so I called it that.'[9]

I caught up with White to ask him about his interaction with de Guzman and his reflections on how cyber crime has evolved in the last 20 years. Here is what he had to say:

> 'Onel de Guzman existed at a fascinating inflection point in the evolution of technology; in hindsight his story feels like a bridge from the old world to the new. By 2000, email had become near ubiquitous. Often without realizing it, many of us had become increasingly reliant on this relatively new invention. De Guzman's strike at the heart of it was a foreshadowing of the decades that would follow, in which gifted young tech enthusiasts would find flaws in the tech systems underpinning our society, and exploit them with immensely disruptive consequences.
>
> On the plus side, De Guzman's virus also shone light on the growing army of cyber defenders who, even back in 2000, were showing increasing skill in sharing knowledge

> and responding to threats. These folks became more visible: suddenly, the IT managers were thrust into the spotlight of office life, as they wrestled to deal with the havoc hitting their email servers.
>
> The Love Bug also took place in a moment when regulation around hacking was just starting to emerge in many countries, with the attendant struggles around enforcement. In 2000, in the Philippines where de Guzman lived, there was no law against hacking. As a result, although suspicion swirled around his culpability, he could never be officially blamed – until I tracked him down two decades later.
>
> And that's perhaps the most poignant part of de Guzman's tale; these days, anyone behind such a globally successful attack would probably be seen as a rockstar of the hacking world. They'd probably be hired by a tech security outfit on a lucrative salary (indeed, there were rumours that's what had happened to de Guzman). But, partly because of the era in which his virus was unleashed, de Guzman faded into obscurity, seemingly happy watching the tech revolution sweep across the world, while working on his modest stall in the back of a shopping mall in Manila.'

White makes many interesting points here about the point in time, with cyber security and malware, that de Guzman and ILOVEYOU represent. This virus – and the man who created it – highlighted the incredible global connectivity that society found itself increasingly reliant on, with ILOVEYOU spreading around the world to a far greater extent than even de Guzman had anticipated.

Trojans

A Trojan, or Trojan horse, is a type of malware that disguises itself as legitimate software. Unlike viruses and worms, Trojans do not replicate themselves but rely on deception and social engineering to trick a person into executing them, enabling the virus to infiltrate and compromise a computer system. The name 'Trojan horse' is, of course, a reference to the ancient myth in which Greek soldiers concealed themselves inside a large wooden horse to gain access to the city of Troy.

Trojans often masquerade as harmless or beneficial programs, such as games, utilities or software updates. Unlike worms or viruses, Trojans do not self-replicate. They rely on human interaction to propagate and so those spreading them have to entice us to download or execute them, believing they are legitimate. Trojans can be distributed through various means, such as email attachments, malicious downloads from websites and software downloads from untrustworthy sources. Trojans carry a hidden malicious payload, which can vary widely from activities such as stealing sensitive data (e.g. usernames, passwords or personal information), creating backdoors for remote access, distributing other malware, or damaging or disrupting the infected system. Common types of Trojans include:

- Banking Trojans, designed to collect online banking credentials or other financial information.
- Spyware Trojans, aiming to spy on computer users, for example watching or tracking us and stealing our personal data.

- Rootkits, designed to gain access to and control over devices.
- Ransomware, which encrypts (locks) data and files, demanding a payment to restore access; ransomware is often spread via Trojans (which are covered in more detail below and in Chapter 10).
- Remote access Trojans (RATs), one of the most powerful forms of malware. RATs enable attackers to gain full administrative rights and remove control of compromised devices.

The 2000s marked the growth of botnets and one of the most famous botnets is a banking Trojan named ZeuS, which infected over 13 million machines since it was first detected in 2007.[10] ZeuS is a multitasker that specializes in two main areas: stealing people's financial information and bringing machines into the botnet, enabling the attack to keep proliferating.

A botnet is a network of compromised computers, known as bots or zombies, with those maliciously controlling them often referred to as the bot herder or botmaster. These compromised computers, also known as infected hosts, most often become part of a botnet without their owners' consent or even knowledge. Botnets are used for various malicious activities, and they can range in size from a few dozen to hundreds of thousands of compromised machines. The bot herder manages the botnet through a central server or a distributed network of servers, known as the command-and-control (C&C) infrastructure. This is where they issue commands to the infected bots. Botnets are designed to be resilient and difficult to dismantle. They can adapt to changes, such as the

removal of infected machines or blocking communication channels with the C&C servers. Botnets can be geographically distributed and may include a mix of different types of devices, including traditional computers, servers, smartphones and Internet of Things (IoT) devices (see Chapter 11 for more on connected devices and botnets).

Vyacheslav Penchukov was a well-known DJ in his Ukrainian hometown of Donetsk. His DJ name was 'DJ Slava Rich', but his hacker handles appear to have been 'father' and 'tank'. In 2022, Penchukov was arrested in Switzerland, having been named in a 2014 US Department of Justice indictment as a leading figure in the JabberZeuS Crew (a cyber crime group). The wanted poster for Penchukov – alongside his associates Alexey Dmitrievich Bron ('thehead') and Ivan Viktorvich Klepikov ('petr0vich' and 'nowhere') – details how the three are wanted for their involvement in a wide-ranging racketeering enterprise that installed ZeuS on victims' machines, captured personal and financial data and used this to coordinate unauthorized funds from victim accounts.[11]

The particular strain of malware being used by the JabberZeuS Crew appears to have been made for them by the alleged author of the original ZeuS Trojan, Evgeniy Mikhailovich Bogachev. Bogachev is also accused of creating and running GameOver ZeuS (GOZ).[12] In 2015, the US State Department and FBI announced the highest bounty US authorities had ever offered in a cyber case at that time: a $3 million reward for information leading to Bogachev's arrest or conviction. He was indicted by a federal grand jury in the US on 22 August 2012, under his handle 'lucky12345', and then again on 19 May 2014 under his

true name, for multiple charges related to his alleged involvement in a 'wide-ranging enterprise and scheme that installed, without authorization, malicious software known as "Zeus" on victim's computers'.[13]

GOZ is a Trojan horse that originally spread via emails that contained links to malicious websites. When victims clicked on the links and visited the websites, malware would infect their computer, drawing the device into the GOZ botnet, which could then be remotely controlled via the malware. The botnet was split into three layers: the bottom layer of infected machines, a middle layer of servers – intended to separate the infected machines and the top layer – and then the highest layer which operated the botnet by issuing commands and receiving stolen data from the infected machines.[14] This decentralized, peer-to-peer infrastructure made it more resilient, described by the US Department of Justice as 'the most sophisticated and damaging botnet we have ever encountered'.[15] GOZ stole bank credentials from victims and operated as a distributor for Cryptolocker ransomware. If this is getting complicated, here's how we can simplify it: the GOZ malware spread via a Trojan horse, controlled via a botnet in order to steal victim's financial data to facilitate fraud. It also worked as a distributor of the Cryptolocker ransomware.

Ransomware

Ransomware is a form of malware that encrypts a victim's data and demands a ransom for decryption. The first known instance of ransomware was called the 'AIDS

Trojan' or 'PC Cyborg', created by Dr Joseph Popp and distributed to thousands of people in 1989. The malware was distributed on floppy disks and was activated after the victim's computer had been rebooted 90 times. Once activated, it encrypted the filenames on the victim's hard drive and displayed a ransom note demanding payment.

While the AIDS Trojan was relatively unsophisticated and its distribution method was not as effective as modern ransomware, it laid the foundation for the ransomware attacks we have seen grow exponentially in recent years. Ransomware has evolved, with various strains emerging, each using different encryption techniques and tactics to extort money from victims.

Cryptolocker emerged as a new variant of ransomware in 2013, affecting Microsoft Windows systems and, like all ransomware, restricted victims' access to infected computers demanding they pay a ransom for access to their data to be returned (Chapter 10 is dedicated to the topic of ransomware but, given the relationship between Cryptolocker and GOZ, it is important to touch on this here). It ran until May 2014, and together with the GOZ botnet, infected between 500,000 to one million computer systems, generating financial losses over £100 million in the US alone.[16] As well as being propagated via the GOZ botnet, it also spread via malicious email attachments on phishing emails.

In June 2014, the US Justice Department announced that an international law enforcement operation – the biggest of its kind at the time – had succeeded in seizing control of the GOZ botnet and disrupting Cryptolocker. A multi-national effort of law enforcement, security firms

and academics from over 10 countries worked together to seize the botnet, battling the complexity of the decentralized structure. The UK's National Crime Agency (NCA) warned at the time that people probably had about two weeks before the criminals would revive the botnet, advising people how to identify if their computer was infected and steps to protect their devices. Bogachev was then added to the FBI's Most Wanted list for his alleged role as the leader of the Russian cyber crime gang operating this malware, with a record-breaking reward sum offered for information.

Before the GOZ botnet was even seized, Cryptolocker copycat ransomware had already emerged, including Locker and Cryptolocker 2.0. This is not surprising: since 2020, researchers have identified over 130 different strains of ransomware in the wild.[17]

Malware-as-a-Service

In the history of JabberZeuS, ZeuS and GameOver ZeuS, I mentioned the allegation that Bogachev made the JabberZeuS malware for Penchukov and his associates. This is not surprising when viewed in the context of Malware-as-a-Service (MaaS). MaaS is a 'business model' whereby cyber criminals who create malware then provide access to that malicious software, and the infrastructure to run it, to other individuals and groups for a fee. Emerging as a trend in the 2010s, this lowered the technical bar to entry into the lucrative world of cyber crime, enabling cyber criminals to rent or purchase malware tools and services on the dark web. It's a way for individuals or

groups with limited technical skills to access and deploy malware for malicious purposes and for those with the skills to increase their return on investment, scaling up their operations while reducing their risk by selling or renting malware, rather than running it themselves. MaaS is one of the reasons we have seen such a huge growth in cyber crime in the last decade or so, with the commoditization of cyber crime.

MaaS gives us an insight into the extent to which cyber crime has become a professional enterprise for many criminals. MaaS providers offer a wide range of malicious software, including banking Trojans, keyloggers, botnets and more. These tools can be tailored for different purposes, from stealing personal information to conducting distributed denial-of-service (DDoS) attacks. The most common form of MaaS is ransomware, with research suggesting Ransomware-as-a-Service (RaaS) made up 58 per cent of MaaS from 2015 to 2022[18] (for more on RaaS, see Chapter 10). MaaS providers typically offer various payment models to their 'customer', such as one-time fees, subscription-based services, or revenue-sharing arrangements where the MaaS provider takes a percentage of the ill-gotten gains from successful attacks. Just like legitimate software, MaaS offerings often include updates, technical support, and even customer service to assist users with any issues they encounter while deploying the malware.

As Hyppönen says – and I hope this chapter illustrates – malware outbreaks like ILOVEYOU are gone, part of a more innocent time in the history of the internet and technology. We live in a very different age now, where the malicious element of malicious software can be jaw-dropping.

Spyware

As time has gone on the malevolence of malware has become much more marked – and it is hard to think of malware that is more insidious than spyware. Spyware is, as the name suggests, spying software that secretly gathers information on the computer user (and for the purposes of this discussion, I am not including adware, which monitors data to inform advertising purposes, and instead focusing on spyware that is used for more malicious, illegitimate purposes). Spyware infiltrates your device (for example via an app, malicious website or malicious attachment), then monitors and captures data (such as email addresses, usernames, passwords, credit card data and keystrokes) before sending the stolen data back to whoever installed, and is operating, the spyware.

Spyware was at the centre of an international scandal that hit the headlines in 2020, involving two of the richest, most powerful men on Earth. In February 2019, Jeff Bezos published an article in which he accused the National Enquirer of trying to blackmail him with photographs, after the National Enquirer had alleged Bezos was engaged in an extra-marital affair. Almost a year later, in January 2020, reports emerged that Jeff Bezos' smartphone was hacked by the Crown Prince of Saudi Arabia via a video sent over WhatsApp in May 2018, infecting the phone with Pegasus spyware. It was alleged that the video, sent by Prince Mohammed to Bezos, hid Pegasus spyware which transmitted large amounts of data from Bezos' phone within hours of receipt. This brought awareness of

both spyware and the vulnerability of phones (those computers that we take everywhere with us) into the mainstream.

Why would Saudi Arabia want to hack Jeff Bezos, the billionaire owner of Amazon? Not for his role at Amazon, or because he was the richest man in the world, but rather the motive was tied to his role as the owner of *The Washington Post*, which had published a series of columns by the journalist Jamal Khashoggi that were critical of the Saudi regime and the Crown Prince.[19] When Khashoggi was murdered in October 2018, *The Washington Post* increased its criticism of the regime.

This incident highlights the changes we have seen with malware over the last two decades or so and answers two questions I am often asked about malware: does it infect phones as well as computers, and is Apple as susceptible as Microsoft and Android devices? Cyber criminals are attracted by a good return on investment and so the more we have embraced Apple devices and the more we have used smart phones and tablets as minicomputers, the more they seek to buy, build and develop malicious software that exploits these platforms. Apple devices use a closed ecosystem, meaning that only approved software can be installed on Apple devices, with a strict review process for the App Store limiting malware from being spread by masquerading as legitimate apps. However, nothing is 100 per cent and the more we use certain technologies, platforms and devices, the more cyber criminals will seek to find and exploit their vulnerabilities.

Protecting against malware

What started as edge experiments to test skills – to see whether the technical ability of the few could exploit the vulnerabilities of new technology – has morphed into theft, espionage and exploitation at a global scale. Cyber crime operates at an industrial scale with personal, professional and political dimensions that few anticipated.

Although malware has grown phenomenally in scale, application and financial gain for cyber criminals, this does not mean that we cannot take steps to defend ourselves. Following foundational cyber security steps can help protect your devices, including:

1 Keep software and devices updated: these updates often include security patches that address newly found vulnerabilities exploited by malware. Enable automatic updates whenever possible to ensure you're protected against the latest threats, as once the vulnerabilities have been found, it's highly likely that cyber criminals are at least attempting to exploit them.
2 Be wary of social engineering: as addressed in *Phishing*, Chapter 1, exercise caution when opening email attachments or clicking on links in emails and messages, especially if they are unexpected. As the examples in this chapter remind us, malicious attachments and links can infect systems and devices with malware.
3 Install anti-virus software and keep it up to date: these programs can detect and remove many types of malware. Ensure that real-time scanning is enabled, and schedule regular scans of your system.

4 Browse the internet mindfully: be conscious of the websites you visit. Stick to trusted, well-known sites, and avoid downloading files or clicking on links from unknown sources. Use a web browser that has built-in security features.
5 Protect your online accounts: passwords should not be based on known words and phrases, as these are easily cracked. Avoid using the same password for multiple accounts and consider using a reputable password manager to help you generate and store these unique, complex passwords. Adding a double-layer of security with multi-factor authentication means that the security of your online accounts is not reliant on passwords alone. See Chapter 2 for more on this.
6 Back up your data: regularly back up your data – and test the backups are working as you would expect – on an external drive or secure cloud service. In the event of a malware infection, backups can help you restore your data and your system without losing valuable information or resorting to paying a ransom.

Notes

1 Hamilton, I (2022) Mark Zuckerberg's new values for Meta show he still hasn't truly let go of 'move fast and break things', Business Insider, 16 February. www.businessinsider.com/meta-mark-zuckerberg-new-values-move-fast-and-break-things-2022-2 (archived at https://perma.cc/L22E-GV7D)
2 Kaspersky (2023) A brief history of computer viruses & what the future holds. usa.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds (archived at https://perma.cc/XBG3-58TZ)

3 Malicious Life Podcast (2021) The Melissa virus. youtu.be/-KrjPxBygz4?si=wzBFoUr5DoTiWWDG (archived at https://perma.cc/E3GK-ZBXJ)
4 Ibid
5 US General Accounting Office (1999) The Melissa computer virus demonstrates urgent need for stronger protection over systems and data, Testimony before the Subcommittee on Technology, Committee on Science, House of Representatives, 15 April. www.govinfo.gov/content/pkg/GAOREPORTS-T-AIMD-99-146/pdf/GAOREPORTS-T-AIMD-99-146.pdf (archived at https://perma.cc/C966-TFN2)
6 FBI (2019) The Melissa virus: an $80 million cyber crime in 1999 foreshadowed modern times. www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519 (archived at https://perma.cc/3MQQ-PH44)
7 US General Accounting Office (1999) The Melissa computer virus demonstrates urgent need for stronger protection over systems and data, Testimony before the subcommittee on Technology, Committee on Science, House of Representatives, 15 April. www.govinfo.gov/content/pkg/GAOREPORTS-T-AIMD-99-146/pdf/GAOREPORTS-T-AIMD-99-146.pdf (archived at https://perma.cc/2W58-SVCF)
8 Winder, D (2020) This 20-year-old virus infected 50 million Windows computers in 10 days: why the ILOVEYOU pandemic matters in 2020, Forbes, 4 May. www.forbes.com/sites/daveywinder/2020/05/04/this-20-year-old-virus-infected-50-million-windows-computers-in-10-days-why-the-iloveyou-pandemic-matters-in-2020/ (archived at https://perma.cc/LLG6-DR2X)
9 White, G (2020) *Crime Dot Com: From viruses to vote rigging, how hacking went global*, TJ International, Cornwall, UK, p 30
10 Balaban, D (2022) The 8 biggest botnets of all time, Cybernews, 18 May. cybernews.com/security/the-8-biggest-botnets-of-all-time/ (archived at https://perma.cc/H26X-UBYN)
11 FBI most wanted JABBERZEUS SUBJECTS. www.fbi.gov/wanted/cyber/jabberzeus-subjects (archived at https://perma.cc/K6BX-546B)
12 Krebs, B (2022) Top Zeus botnet suspect 'tank' arrested in Geneva, KrebsonSecurity, 15 November. krebsonsecurity.com/2022/11/top-zeus-botnet-suspect-tank-arrested-in-geneva/ (archived at https://perma.cc/9P58-49QA)

13 FBI (n d) FBI most wanted EVGENIY MIKHAILOVICH BOGACHEV. www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev (archived at https://perma.cc/Y426-LX4B)
14 Andriesse, D et al (2013) Highly resilient peer-to-peer botnets are here: an analysis of Gameover Zeus, 8th International Conference on Malicious and Unwanted Software: The Americas (MALWARE). IEEE. ieeexplore.ieee.org/document/6703693 (archived at https://perma.cc/S7J9-RPCB)
15 Cole, J (2014) Deputy Attorney General James Cole deliver remarks at press conference for Gameover Zeus and Cryptolocker Operations, Office of Public Affairs US Department of Justice, 2 June. www.justice.gov/opa/speech/deputy-attorney-general-james-cole-delivers-remarks-press-conference-gameover-zeus-and (archived at https://perma.cc/VGQ5-X2PJ)
16 US Department of Justice (2014) US District Court for the Western District of Pennsylvania Complaint, 27 May. www.justice.gov/sites/default/files/opa/legacy/2014/05/30/complaint.pdf (archived at https://perma.cc/2VFY-XX4G)
17 IBM (2023) What is ransomware? www.ibm.com/topics/ransomware (archived at https://perma.cc/Z7YQ-RPXH)
18 Kaspersky (2023) 58 percent of malware families sold as a service are ransomware. www.kaspersky.com/about/press-releases/2023_58-percent-of-malware-families-sold-as-a-service-are-ransomware (archived at https://perma.cc/K3EN-TVW4)
19 Kirchgaessner, S (2020) Revealed: the Saudi heir and the alleged plot to undermine Jeff Bezos, The Guardian, 21 January. www.theguardian.com/world/2020/jan/21/revealed-the-saudi-heir-and-the-alleged-plot-to-undermine-jeff-bezos (archived at https://perma.cc/4FCR-85XM)

CHAPTER TEN

Ransomware

Although ransomware first emerged in 1989 with the AIDS Trojan aka PC Cyborg, it wasn't until the 2010s that this form of malware became a real cyber security headache, and even then, we had little idea of the ransomware migraine that awaited us in the 2020s.

In 1989, the AIDS Trojan spread via floppy disk and demanded $189 be sent to a PO box in Panama for the system to be restored. In 2013, Cryptolocker (which we looked at in the previous chapter) was named the most malicious malware, demanding $750 to be paid by MoneyPak (where cash can be sent to prepaid cards) or Bitcoin.[1] In September 2023, Caesars Entertainment confirmed a cyber security incident in an SEC filing, with reports suggesting that they paid a $15 million ransom, after negotiating with

the cyber criminals responsible to bring their demand down from the original request of $30 million.[2]

Average ransomware payouts over the years show how this problem has exploded:

- 2012 – $200[3]
- 2014 – $373[4]
- 2015 – $294[5]
- 2016 – $1,077[6]
- 2020 – $303,756[7]
- 2021 – $541,009[8]
- 2022 – $812,380[9]
- 2023 – $1,542,333[10]

In 2023, ransomware hit record levels with over 500 major incidents in July and then again in September.[11] Lindy Cameron, CEO of the UK National Cyber Security Centre, has described it as 'the biggest global cyber threat'.[12] How did we get to this point?

Cryptocurrency

When ransomware first emerged, criminals demanded their ransoms be paid either via Western Union or prepaid cards such as MoneyPak. These routes did not scale well and, although not as easy to trace as cash, they were still traceable. The availability of Bitcoin and other cryptocurrencies aligns with the prolific rise of ransomware. Research also highlights a correlation between the price of Bitcoin and the number of ransomware attacks: data shows a lesser number of ransomware attacks correlating with a lower price of Bitcoin.[13]

Cryptocurrency is decentralized and unregulated, using blockchains – distributed ledgers – to register and track transactions. While the movement of cryptocurrency can be traced (as we will cover in detail in Chapter 12), it is much more challenging to trace than traditional currency, offering layers of anonymity. Cyber criminals generally route illegitimate funds, such as ransomware payouts, through a layered process of unregulated financial entities in a bid to hide their tracks and receive the funds without an identifiable link to themselves. When the ransom payment is made to a cryptocurrency wallet,* criminals will use multiple tactics to hide the journey of the funds. These methods include chain hopping, in which one form of cryptocurrency is exchanged for another using multiple cryptocurrency exchanges, and the use of mules. Cyber criminals also use mixers, companies which offer services to jumble up cryptocurrency to help conceal who owns which cryptocurrency units. When I interviewed Benedict Hamilton about his experiences investigating cryptocurrency crime, we spoke about the extent to which cryptocurrency contributed to the growth in ransomware and financially motivated organized cyber crime in general. This is what he had to say:

> 'Everyone has to admit that without crypto, it would be a lot more challenging for ransomware and crime. Ever since Capone or earlier, the way governments have tried to fight organized crime is by putting regulation and responsibilities

*The software that stores, sends and receives cryptocurrency.

> on the banks. Crypto offers a way through that for cyber criminals, even more so when they avoid regulated exchanges.'

Bitcoin was the first cryptocurrency, and it remains the most commonly demanded cryptocurrency in ransomware attacks, with research suggesting Bitcoin is used for ransomware payouts in 99 per cent of cases.[14] The criminals want their victims to pay the ransom – often providing detailed instructions on how to acquire Bitcoin, alongside other 'customer support' information – and so choosing a cryptocurrency that is universally known and easy to acquire is only logical. However, there is a small but increasing trend of criminals demanding payment with privacy coins such as Monero (or giving victims the 'option' to pay with Monero, often at a discounted rate), which have privacy built into them as a native function. Monero is built on its own blockchain with privacy features that hide the sender, receiver and the amount being sent; unlike Bitcoin, where all transaction details are transparent and public, Monero transactions are designed to be confidential and untraceable. If an organization pays a ransomware demand via Monero, that transaction will be less visible, bringing less scrutiny to the transaction as well as less ability for investigation and recovery of funds. Although recovering cryptocurrency funds after a ransomware payout is rare, it is not unheard of.

Colonial Pipeline is the largest pipeline system for refined oil in the US, running 5,500 miles long and provides approximately 45 per cent of the fuel for the East Coast of the country. On 7 May 2021, Colonial Pipeline Co. was

forced to shut down the pipeline for six days following a ransomware attack, which prompted a run on gasoline, pushing prices to the highest point in over six years and leaving many gas stations empty. The Biden administration issued an emergency declaration in 17 states as it attempted to deal with the fuel crisis.

The cyber crime group DarkSide issued an unprecedented apology for the attack that was allegedly carried out by their affiliates, stating that in future they would check each company that their affiliates were targeting to avoid social consequences, as their 'goal is to make money, and not creating problems for society'.[15]

One month following the attack, Joseph Blount, CEO of Colonial Pipeline Co., told a US Senate Committee that they had made the difficult decision to pay a ransom of $4.4 million to DarkSide to be able to restore operations as soon as possible, after the criminals were able to infect the Colonial Pipeline Co. systems by exploiting a legacy virtual private network (VPN).[16] Reports suggest that the criminals gained access to the system with a compromised username and password found on the dark web – notably, there was no multi-factor authentication in place.

There are many lessons we can learn – and that authorities and organizations have taken – from the Colonial Pipeline ransomware attack. An optimistic lesson which emerged from the incident is that cryptocurrency funds can be recovered in some cases: one month after the attack, the US Department of Justice announced seizure of approximately 85 per cent of the ransom paid.[17] Officials declined to comment how they had tracked the funds through at least 23 electronic accounts belonging to the DarkSide

group, before seizing 63.7 of the 75 Bitcoins paid in ransom.

In the wake of the Colonial Pipeline attack in May 2021, President Biden said that the United States would not rule out a retaliatory strike against DarkSide to 'disrupt their ability to operate'; shortly after this, DarkSide announced it was shutting down its affiliate operation in a Russian statement on its website which cited 'pressure' from the United States, saying it had lost access to its blog and payment server and that funds had been withdrawn to an unknown account.[18]

An evolving ransomware business model

DarkSide ran like a sophisticated enterprise; one of a cluster of cyber crime groups to do so. Operating out of Eastern Europe (thought to be Russia), they provided Ransomware-as-a-Service (RaaS). Alongside the (perception of) anonymity of cryptocurrency, the RaaS business model is one of the reasons that ransomware is such a huge, global cyber security threat. 'Affiliates' pay a fee to ransomware operators to launch an attack using their malware and infrastructure, meaning the technical barrier to entry for cyber crime has been massively lowered. Operators, such as DarkSide, sell their RaaS kits on the dark web and many include features such as 24/7 support, monthly payment and profit-sharing models, dashboards for operating and tracking the attacks, victim payment portals and victim payment negotiation support.

RaaS operators are structured like successful businesses, with hierarchies of 'employees' working in different functions, from sales to negotiations to customer support. They place job adverts on the dark web, detailing the technical skills they are looking for, hiring for specific roles that call for malware specialists, credential theft and vulnerability hunting. A small group of ransomware gangs function as RaaS operators and it seems that they interview prospective members and partners, much in the same way as legitimate businesses.

Big game hunting in ransomware

The evolution of ransomware highlights the extent to which cyber crime is now big business. Until the mid-2010s, ransomware was automated and the criminals behind it were focused on hitting lots of smaller targets for lower sums. Phishing emails with malicious attachments were sent out in 'spray and pray' style attacks, where criminals would rely on enough people infecting their systems via the malicious attachments to pay the few hundred dollars in Bitcoin each. Up until 2017–18, ransomware largely hit home computer users and small businesses were the most common victims. It seemed a sneaky and successful approach: go for the low-hanging fruit with spray and pray automated attacks, attaching a low fee to the ransom, and bank on the fact that enough people will pay to get their data back to make the effort more than worthwhile. But then, some ransomware gangs realized they could hunt lions, not just mice, and make a much greater return on investment. Rather than only aiming at smaller targets for

lower ransom demands, they could seek out the big fish, for much greater ransom payments. Ransomware gangs pivoted towards targeting large corporations that are more likely to pay a huge sum if their operations come to a screeching halt with a ransomware attack.

Switching from automated ransomware campaigns to human-operated ones, the attackers could also embed themselves more deeply in a network and move laterally through an organization to get greater command and control. This approach is less noisy and more nuanced, so the attackers could look for valuable data enabling them to pivot their tactics away from simply encrypting data and into double extortion methods. Analysis shows that ransomware operators have extorted at least $449.1 million from January to June in 2023, putting them on track for their second most lucrative year.[19]

However, this does not mean that smaller targets are impervious to ransomware, with data showing that many ransomware gangs still successfully focus on small attacks, with RaaS strains Dharma, Phobos and Stop/djvu used in unsophisticated spray and pray attacks against smaller targets, with average payouts for these strains in 2023 ranging from $265 to $1,719.[20]

Escalating extortion

The gangs realized that they could scale-up their operations: with RaaS, bigger targets and by changing the ransomware rules of engagement, pivoting to double extortion in big targets. Rather than simply encrypting a

victim's data, they began also stealing it and threatening to leak it if the ransom is not paid.

In November 2019, Maze ransomware group breached Allied Universal, a security firm with 200,000 people and revenues over $7 billion. Maze downloaded Allied Universal data and then executed ransomware in their network, before demanding a $2.3 million ransom in return for a promise that they would share the decrypter and keep their data safe. They threatened Allied Universal that if the ransom was not paid, they would contact the tech news site Bleeping Computer with proof of breach before making the stolen data public; they followed through with their threats, first contacting Bleeping Computer and then publishing almost 700 MB of sensitive data stolen from Allied Universal the night before the deadline.[21] Maze went on to make their data leak architecture available to other attackers. The double extortion tactic began to dominate ransomware attacks; within a year, 15 different ransomware groups were using the same approach.[22]

Maze displayed further 'business' acumen when they went on to launch a Maze News site on which they published the data of their victims who did not pay together with press releases. They also – alongside other ransomware gangs – continued to up the ante in the summer of 2020, when they started cold-calling victims who were in the middle of an attack but had not yet paid. Signs indicated that multiple groups were sharing a call centre that was outsourced to communicate scripted phone calls with victim companies, prompting them to 'stop wasting your time and recover your data'.[23]

Law enforcement whack-a-mole

In September 2020, Maze halted attacks on new victims and began shutting down their operations. On 1 November 2020, they shut down their website stating 'Maze Team Project is announcing it is officially closed', claiming that they never had partners or successors and their specialists do not work with other software. Ever 'professional', the announcement indicated that victims who want their information to be deleted should contact the group within a month, failing to include that the group would of course still expect payment and offering no guarantee that they would keep to their word and actually delete the data.

The Maze announcement went on to blame the victims of their attacks, offering an apparent justification for their ransomware activities:

> 'If you are taking responsibility for other people's money and personal data then try to keep it secure. Until you do that there will be more projects like Maze to remind you about secure data storage.'

They made no mention of the profit they made from these attacks, nor the distress caused to the people working in those companies, their customers, suppliers and partners. Before Maze was even shut down, affiliates had moved to a new ransomware operation called Egregor, which appeared to be Maze by another name. After six months, it was estimated that the Maze/Egregor group had made $80 million from a criminal enterprise that victimized 150 companies before being disrupted by an international law enforcement operation.[24] Law enforcement from Ukraine,

France and the US worked in collaboration to shut down the Egregor leak website, seize computers and arrest individuals, many of whom were suspected of being affiliates but at least one of whom may have been at the top of the Egregor RaaS food chain.[25]

This is a familiar pattern with ransomware operators: when law enforcement's attention becomes too loud and uncomfortable, the gangs 'retire', generally emerging again within a short space of time under a new name. They also work in partnerships, bringing together different elements from previous groups. When DarkSide announced it was shutting down its affiliate operation in May 2021 after the attack on Colonial Pipeline, the hiatus lasted less than a couple of months before the operation returned as BlackMatter in July. Within four months, the cyber security company Emsisoft had created a decrypter, meaning victims could recover their files without considering whether to pay the ransom. DarkSide/BlackMatter then seemingly relaunched under the ALPHV/BlackCat brand in November 2021, with members of the latter confirming they used to be connected to the DarkSide/BlackMatter operation as well as REvil and Maze/Egregor.[26]

Borders in a borderless crime

With the disbanding of DarkSide citing pressure from the US, the action against Maze/Egregor and the occasional international arrest of cyber criminals, the obvious question is: why is law enforcement not *more* successful in disbanding and apprehending these criminal enterprises?

A cyber attack can spread around the world in minutes. The infrastructure of the internet is global by design and the decentralized nature of cryptocurrency allows for funds to be moved around the world, including profits from cyber crime. Before the advent of connected technology, crime was generally localized, with the perpetrator and victim in the same place, but with cyber crime the perpetrator and the victim are often on different sides of the world. While cyber crime is borderless, efforts to tackle it are either aided or impeded by the relationships between different countries.

Attribution is a common challenge in cyber attacks. Identifying who is behind the code is often very difficult, if not impossible. Tracing attacks through the flow of cryptocurrency is challenging, as Hamilton explains:

> 'In the case of the big ransomware groups, you get quite sophisticated money laundering with very thin profiles attached to all of the records involved in the process and the amount of discovery orders, subpoenas – however you get the information from the exchanges, the amount of analysis that needs to be done – it's a very significant effort and that's why it's done against the groups that will have most impact removing them.'

However, even when the perpetrators have been identified and evidence is clear, taking legal action on those criminals often comes down to matters of jurisdiction. If the person – or group – committing the crime is not within the country or legal jurisdiction of the court, then there is no legal ability for the victim's country to arrest or prosecute the perpetrator. Many countries have established reciprocal

legal rules with allies when it comes to cyber crime, but the West does not have such agreements with China or Russia.

It is commonly understood that criminal hackers in Russia are given free rein by the state, as long as they do not attack Russian citizens. Indeed, this goes beyond the Russian state simply turning a blind eye to cyber crime being conducted on its shores, with the government actively sponsoring some of the activity. In April 2021, the United States Treasury Department acknowledged this connection, stating:

> 'To bolster its malicious cyber operations, the FSB cultivates and co-opts criminal hackers, including the previously designated Evil Corp, enabling them to engage in disruptive ransomware attacks and phishing campaigns.'[27]

Evil Corp emerged in the late 2000s, they are based out of Russia and regarded as one of the most capable cyber crime organizations in the world. They developed Dridex (also known as Bugat) malware, as well as BitPaymer and WastedLocker ransomware variants, operating with impunity for at least a decade and becoming known as 'some of the most infamous and flashiest hackers on the planet'.[28] Evil Corp spread Dridex with phishing emails, attacking hundreds of banks and financial institutions across 40 countries to steal over $100 million.

Compromising a wide range of targets, Evil Corp have attacked companies in the healthcare, non-profit, education, finance, government, media and manufacturing sectors. In December 2019, Maksim Yakubets (aka 'aqua' and 'aquamo') was named leader of Evil Corp, alongside Igor Turashev as a member of the gang, in a collaborative

law enforcement effort between the UK and the US. The UK's National Crime Agency posted a Twitter thread sharing the FBI wanted poster for Yakubets alongside multiple photos of Evil Corp members with piles of cash, exotic animals and luxury cars – including a photograph of Yakubets talking to a Russian police officer while next to his customized Lamborghini with a number plate that translates to 'Thief'.[29]

The US is the victim of 43 per cent of all global ransomware attacks, and the UK is next in line.[30] In the US, the average ransom payment at the time of writing (in October 2023) is $2,179,457.[31] Meanwhile, more Russian individuals and organizations have been sanctioned and indicted by the West than those of any other nationality. With the UK and the US joint effort to tackle Evil Corp, Yakubets and Turashev became the latest Russian individuals to be named as cyber criminals by the US Government, sanctioned (freezing any Western assets that they hold and barring them from doing business with Western firms) and indicted (banning them from travel).

Sanctions have become a core part of the Western response to ransomware, but a core question is yet to be determined: do they work? When I interviewed Pete Cooper, former deputy director for the UK Cabinet Office, we explored this question. Here is what he had to say:

> 'One of the key challenges with sanctions against threat actors is, how much do they care when they're outside extradition reach? And, what is the tangible measure of success that sanctions give you over the long term? We've got a lever but we don't know if it's working or not.'

On top of the indictments and sanctions, a $5 million bounty was offered for information leading to Yakubets' arrest, topping the record-breaking sum that was offered for Bogachev in 2015. It is not surprising that before leading Evil Corp, Yakubets was associated with Bogachev, who we met in the previous chapter as the cyber criminal responsible for ZeuS, JabberZeuS and GameOver ZeuS. Both are believed to have worked for the Russian FSB.

The relationship between the Russian state and their homegrown criminal enterprises is why the response to the ransomware attack on Kaseya in 2021 was so surprising.

At the start of the Fourth of July weekend in 2021, a ransomware attack on software provider Kaseya was estimated to affect thousands of other organizations around the world, after criminals breached Kaseya via a zero-day vulnerability in a remote computer management tool (for more on zero days, see Chapter 3). In the days following attack, the RaaS group REvil (short for Ransomware Evil) boasted that they had launched the attack on Kaseya, resulting in one million systems being infected. They placed the price of decryption at $70 million in Bitcoin, promising that this would unlock all of the data they were holding hostage. The incident was described as the biggest global ransomware attack on record, with victims on all continents and in sectors spanning financial services, the public sector, IT services and more, with 800 Swedish Co-op grocery stores having to close because their cash register software supplier could not function.[32] Many small businesses such as dentists, architecture firms and libraries were impacted, reliant on Kaseya as their IT service provider.

REvil was believed to be a Russian RaaS operation, who claimed to make an annual revenue of $100 million. As well as the attack on Kaseya, they were also responsible for ransomware attacks on meat supplier JBS and on Quanta Computer, an Apple supplier, which enabled them to steal Apple blueprints. Highlighting the strategic approach taken by many of these gangs, REvil seemingly adjusted their ransom request based on the annual revenue of the victim organization. The REvil ransomware was one of the most prominent in 2021 and as such, in November 2021, the US Department of State offered a reward of up to £10 million for information leading to REvil gang members.

In January 2022, Russian authorities stated that they had dismantled REvil and charged 14 members of the group, halting their operations and seizing millions of roubles, some cryptocurrency and luxury cars. The Russian authorities stated that they had made the arrests using information provided by US authorities, with the operation marking the first time in years that the US and Russia collaborated on a cyber crime operation.

Three months later, in April 2022, the old REvil victim site came back to life, forwarding to a new site that featured old and new victims as well as a recruitment advert for new affiliates that promised a new, improved version of the previous REvil ransomware.

This tendency of ransomware operations to rebrand when it is convenient for them causes another tension with the use of sanctions, which restrict companies in the country issuing the sanction from transferring funds to those

who have been sanctioned. As Cooper said in our conversation:

> 'As the victim, understanding the layers below the attack of "who" has ransomwared you is hard. Are they sanctioned? If you pay, are you breaking the law? Would anything happen if you did? We are only at the start of understanding the long-term legal complexity.'

Insurance, brokers and negotiators

Steve Haase, an insurance broker and senior vice president at Hamilton Dorsey Alston Co, worked for two years to persuade colleagues in the insurance industry to back a new product to protect companies whose data was stolen from their computers and in 1997, he finally succeeded.[33] Cyber insurance was born. In 2021, global premiums reached $10 billion, and the market is expected to grow to £23 billion by 2025.[34]

On the face of it, cyber insurance is simple: the insurance industry sells policies to organizations to cover losses in the event of a cyber attack. Policies often include specific coverages for ransomware, including for the payment of a ransom, and data reflects that ransomware accounts for between one-fifth[35] to one-third[36] of all cyber insurance claims.

Cyber insurance is a contentious topic in the cyber security community. On the one hand, policies can not only offer support for victims at the point of attack, even taking on the role of negotiating with the criminals for a lower

payout, they also often require a strong cyber security foundation among their policy holders. This can help security leaders and teams advance the security maturity of their organization, even as a tool to leverage among resistant boards, who may not see the benefit of investing in cyber security until they see it as a requirement on their cyber insurance policy.

On the other hand, is the argument – and evidence – that cyber insurance encourages victim organizations to pay the ransom. A member of the REvil group described in an interview their tactic of hacking the insurance companies to get their list of customers, targeting the list and then hitting the insurer themselves; they described organizations with cyber insurance as 'the tastiest morsels'.[37]

To pay or not to pay, is that the question?

When faced with a ransomware attack, the victim organization must decide whether to pay or not. This is a time of huge pressure, trying to investigate and understand what has happened and what data has been compromised, meanwhile dealing with an impact on business operations which can sometimes reduce an organization to running on pen and paper. At the same time, the organization has to navigate communications with law enforcement, regulators, customers, third parties and perhaps the media. The criminals holding the organization to ransom will be adding more pressure, with a time deadline and communications (even phone calls) with the victim organization as well as partners and journalists. As time ticks on, they will often start

publishing some data to up the ante. Even with support from third parties such as incident response specialists, negotiators, intelligence agencies, law enforcement and cyber insurance companies, it is an extremely challenging time.

Amid all of this, the organization will be determining whether to pay the ransom (unless that decision has been agreed and documented ahead of time) and, perhaps, trying to haggle with the criminals or at least stall their threats. For organizations that deliver a vital service, such as healthcare or as in the Colonial Pipeline case, returning to operations as soon as possible is critical. For others, avoiding a catastrophic loss of revenue, minimizing disruption to business operations and limiting negative PR feeds into the decision.

I would never recommend an organization pays the ransom, but I also would not judge those who do make such a difficult decision, with livelihoods and services to consider. However, paying the ransom fuels the business model and the operations of the criminal gangs, enabling the crime to continue to grow. There is an ethical question to answer here, and legal issues must be addressed, too. With the increasing use of sanctions and legislative moves to further prohibit the payment of ransoms, an organization that is considering paying a ransom must address whether they would be breaking the law themselves if they transfer funds to the criminals that are holding their data hostage.

However, paying the ransom often does not mean an end to the troubles. Research from Cybereason surveyed 1,456 cyber security professionals from organizations in ten countries and found some sobering trends. Almost

three-quarters said their organization had experienced a ransomware attack in the preceding two years and, of those who paid a ransom, only 42 per cent received a restoration of all systems and data, 54 per cent found that systems issues persisted or some data was still corrupted and 80 per cent were victims of a second attack (68 per cent were hit again in less than a month for a higher ransom).[38] Beyond this, with ransomware gangs now stealing a victims' data as well as locking it up, paying the ransom does not guarantee that they will delete the data as promised – after all, we are relying on the promise of criminals.

The real question we need to answer is how to avoid ransomware in the first place, and how to be prepared for an attack if the worst still happens. As Cooper said in our discussion:

> 'Good security and resilience are the only defence we have against ransomware.'

Ransomware mitigations and managing an incident

It is always better to prevent an attack than to need to respond to one. There are many foundational technical measures an organization can implement to help minimize the likelihood and impact of a successful ransomware attack. These include network segmentation, principles of least privilege access and reducing the external-facing attack surface. A key part of prevention is putting in place a robust and tested data backup solution, which should be offline and encrypted, meaning that the organization is not reliant on the perpetrators of a ransomware attack giving

access to the data back. If you have copies, and those copies are safe from attack, then you are not reliant on the actions of the criminals.

Preventing a ransomware attack is not just about technical measures, but also embracing a people-centred approach to security, for example raising awareness of phishing and social engineering.

Logging activity and access allows organizations to both detect malicious activity and plays a vital role in incident response, enabling visibility of the attack and how far it has spread.

A well-maintained and tested incident response and business continuity plan enables organizations to manage an incident as it unfolds and should include procedures for offline communications that do not rely on business infrastructure such as email systems, in case these systems are compromised by the attackers or even entirely shut down. These plans should also take account of legal requirements and wider PR and communication considerations. An incident response and business continuity team should include legal, HR and communications as well as technical and business leadership. Cooper's advice was that transparency is the best approach:

> 'The only option you have is open communication with staff, regulators, law enforcement and so on.'

In the case of Colonial Pipeline, although the organization paid the ransom, it is telling to note that it was able to get systems back online quicker using its own backups rather than using the decryption key from the criminals.[39] Being prepared for an incident is as important as putting the measures in place to prevent one.

Notes

1 Hansberry, A et al (2013) Cryptolocker: 2013's most malicious malware, Boston University. www.cs.bu.edu/~goldbe/teaching/HW55815/cryptolockerEssay.pdf (archived at https://perma.cc/ZEW9-SNUE)

2 Sayre, K (2014) Caesars paid ransom after suffering cyber attack, The Wall Street Journal, 14 September. www.wsj.com/business/hospitality/caesars-paid-ransom-after-suffering-cyber attack-7792c7f0 (archived at https://perma.cc/XW6H-Z98B)

3 CISA (2016) Crypto ransomware, 30 September. www.cisa.gov/news-events/alerts/2014/10/22/crypto-ransomware (archived at https://perma.cc/H9AC-DSPN)

4 Petrosyan, A (2023) Average demanded ransomware payments worldwide 2014–2017, Statista, 25 August. www.statista.com/statistics/696048/ransomware-demanded-payments-world/ (archived at https://perma.cc/G5UZ-PVLX)

5 Stark, J R (2017) Ransomware payment: legality, logistics, and proof of life. listingcenter.nasdaq.com/assets/Ransomware_White_Paper_1.pdf (archived at https://perma.cc/2QM7-QQ6C)

6 Ibid

7 Unit 42 (2022) 2022 Unit 42 ransomware threat report highlights: ransomware remains a headliner, Palo Alto Unit 42, 24 March. unit42.paloaltonetworks.com/2022-ransomware-threat-report-highlights/ (archived at https://perma.cc/XWW2-QMGQ)

8 Ibid

9 Thomas, D (2023) Report: ransomware payouts and recovery costs went way up in 2023, SC Media, 7 August. www.scmagazine.com/resource/report-ransomware-payouts-and-recovery-costs-went-way-up-in-2023 (archived at https://perma.cc/5FHD-Z6FC)

10 Ibid

11 NCC Group (2023) Cyber threat intelligence report. insights.nccgroup.com/l/898251/2023-10-26/31hd657/898251/1698311635OAeu85cZ/Threat_Pulse_freemium__1_.pdf (archived at https://perma.cc/4NRG-F4E4)

12 Palmer, D (2022) Ransomware is the biggest global cyber threat. And the attacks are still evolving, ZDNET, 28 June. www.zdnet.com/article/ransomware-attacks-are-the-biggest-global-cyber-threat-and-still-evolving-warns-cybersecurity-chief/ (archived at https://perma.cc/XA59-6CVX)

13 Moody, R (2022) Does the price of Bitcoin impact ransomware attacks and ransoms? Comparitech, 19 October. www.comparitech.com/blog/vpn-privacy/bitcoin-price-ransomware-attacks/ (archived at https://perma.cc/7AUU-Y88X)
14 Coveware (2019) Ransomware payments rise as public sector is targeted, new variants enter the market. www.coveware.com/blog/q3-ransomware-marketplace-report (archived at https://perma.cc/QLQ7-ZU6V)
15 Lock, S (2021) Colonial Pipeline hackers, DarkSide, apologize, say goal is 'to make money', Newsweek, 11 March. www.newsweek.com/colonial-pipeline-hackers-darkside-apologize-say-goal-make-money-1590327 (archived at https://perma.cc/WDK3-WJUQ)
16 Blount, J (2021) Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline company, hearing before the United States Senate Committee on Homeland Security & Governmental Affairs, 8 June. www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Blount-2021-06-08.pdf (archived at https://perma.cc/Z8SE-U7GM)
17 Wolf, B (2021) Recovery of Colonial Pipeline ransom funds highlights traceability of cryptocurrency, experts say, Thomson Reuters, 23 June. www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/colonial-pipeline-ransom-funds/ (archived at https://perma.cc/S977-RBFK)
18 Schwirtz, M and Perlroth (2021) DarkSide blamed for gas pipeline attack, says it is shutting down, The New York Times, 8 June. www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html (archived at https://perma.cc/3R2F-99GS)
19 Chainalysis Team (2023) Crypto crime mi-year update: crime down 65% overall, but ransomware headed for huge year thanks to return of big game hunting, Chainalysis, 12 July. www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/ (archived at https://perma.cc/75KY-VQRC)
20 Ibid
21 Abrams, L (2019) Allied Universal breached by Maze Ransomware, stolen data leaked, Bleeping Computer, 21 November. www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/ (archived at https://perma.cc/6X3J-FE9T)

22 Pilkey, A (2021) Attack landscape update: Ransomware 2.0, automated recon, and supply chain attacks, F-Secure, 30 March. https://blog.f-secure.com/attack-landscape-update-h1-2021/?_ga=2.244874309.1793370514.1617091149-247904548.1617091149 (archived at https://perma.cc/N8LR-UDDK)
23 Cimpanu, C (2020) Ransomware gangs are now cold calling victims if they restore from backups without paying, ZDNET, 4 December. www.zdnet.com/article/ransomware-gangs-are-now-cold-calling-victims-if-they-restore-from-backups-without-paying/ (archived at https://perma.cc/AG7H-UJWQ)
24 Barth, B (2021) The Egregor takedown: new tactics to battle ransomware groups show promise, SC Media, 18 February. www.scmagazine.com/news/the-egregor-takedown-new-tactics-to-take-down-ransomware-groups-show-promise (archived at https://perma.cc/439J-HTM5)
25 Ibid
26 Smilyanets, D (2022) An ALPHV (BlackCat) representative discusses the group's plans for a ransomware 'meta-universe', The Record by Recorded Future News, 3 February. therecord.media/an-alphv-blackcat-representative-discusses-the-groups-plans-for-a-ransomware-meta-universe (archived at https://perma.cc/N3KX-699L)
27 US Department of the Treasury (2021) Treasury sanctions Russia with sweeping new sanctions authority, 15 April. home.treasury.gov/news/press-releases/jy0127 (archived at https://perma.cc/6N4T-5VXF)
28 Cox, J (2022) Beef alert: ransomware group very mad at being associated with lavish Russian hackers, Vice Motherboard, 7 June. www.vice.com/en/article/7k8z4x/lockbit-ransomware-group-evil-corp-beef-alert (archived at https://perma.cc/XF8M-UAX8)
29 National Crime Agency (2019) An international law enforcement operation has exposed the world's most harmful cyber crime group, Evil Corp, 5 December. x.com/NCA_UK/status/1202618928209498114?s=20 (archived at https://perma.cc/XQN7-5LQX)
30 Malwarebytes (2023) 2023 State of ransomware. www.malwarebytes.com/blog/threat-intelligence/2023/08/global-ransomware-attacks-at-an-all-time-high-shows-latest-2023-state-of-ransomware-report (archived at https://perma.cc/87AC-QDYJ)

31 Comparitech (2023) Map of US ransomware attacks (updated daily). www.comparitech.com/ransomware-attack-map/ (archived at https://perma.cc/GB9J-9UA2)
32 CBS News (2021) Hackers demand $70 million to end biggest ransomware attack on record, CBS News, 6 July. www.cbsnews.com/news/ransomware-attack-revil-hackers-demand-70-million/ (archived at https://perma.cc/C9BM-9J3V)
33 Wolff, J (2022) A brief history of cyber insurance, Slate, 30 August. slate.com/technology/2022/08/cyberinsurance-history-regulation.html (archived at https://perma.cc/EC8L-858K)
34 Swiss Re Institute (2022) Cyber insurance: strengthening resilience for the digital transformation. www.swissre.com/dam/jcr:6fd9f6dd-4631-4d9f-9c3b-5a3b79b321c0/2022-11-08-sri-expertise-publication-cyber-insurance-strengthening-resilience.pdf (archived at https://perma.cc/Q22Q-FEKK)
35 Hendricks, C (2023) Embracing collaboration amid spike in cyber claims, Coalition, 25 September. www.coalitioninc.com/blog/2023-cyber-claims-report-update (archived at https://perma.cc/W4E7-NDBR)
36 NetDiligence (2023) Cyber claims study. netdiligence.com/cyber-insurance-claims-study/ (archived at https://perma.cc/V98J-FJGA)
37 Smilyanets, D (2021) I scrounged through the trash heaps… now I'm a millionaire: an interview with REvil's Unknown. The Record by Recorded Future, 15 March. therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown (archived at https://perma.cc/BRT7-SP4T)
38 Cybereason (2022) Ransomware: the true cost to business. www.cybereason.com/hubfs/dam/collateral/reports/Ransomware-The-True-Cost-to-Business-2022.pdf (archived at https://perma.cc/RX78-V83A)
39 Arcserve (2021) What the DarkSide ransomware attack can teach us about cyber security and resilience, Arcserve, 22 June. www.arcserve.com/blog/what-darkside-ransomware-attack-can-teach-us-about-cybersecurity-and-resilience (archived at https://perma.cc/GNV7-ECV3)

CHAPTER ELEVEN

Internet of Things (IoT)

In 2016, over 175,000 websites around the world suffered a distributed denial of service (DDoS) attack. Large swathes of the internet in eastern United States and across Europe suffered. Behind it all, was some malicious software (malware) called Mirai.

Speculation abounded that this was the work of a nation, perhaps linked to the looming elections in the US. The attack was claimed by hacking groups Anonymous and New World Hacking – presumably not wanting a crisis to go to waste – who asserted that they were taking revenge for Julian Assange being without internet access in the Ecuadorian embassy.[1] As this attack took huge amounts of the internet offline for many people, the motivation seemed to line up with the impact.

The true story of Mirai is, in fact, far more fascinating.

The story of Mirai illustrates one of the main facets that I love about working in cyber security. It is the human stories lying beneath the technology which never fail to fascinate me.

But, before we get to the full story of Mirai, let's address some technical foundations to paint a full and clear picture of what happened here.

A distributed denial of service, or DDoS, is one of the oldest types of cyber attack. On 6 September 1996, the internet provider Public Access Network Corporation (Panix) was taken offline by the first reported DDoS.[2]

To understand a distributed denial of service, we must first understand a denial of service (DoS). A DoS is when one computer, with one internet connection, overwhelms a website or system with so much internet traffic that the website or system can no longer function. A DDoS is the same, but the overwhelming traffic comes not from one computer and one internet connection, but rather from multiple computers and connections. They are not always malicious: if you have ever been unable to reach a website because of a huge surge in the popularity of that site, you have seen a (non-malicious) DDoS in action. In fact, you've been part of it, because your computer and connection has been one of too many trying to reach that site. A common example: highly anticipated concert tickets are released at a specific date and time, and so many people are keen to book their ticket that the website simply cannot cope with demand.

However, DDoS incidents are also weaponized online and used maliciously. As in the case of Mirai.

Malicious DDoS attacks generally make use of botnets. A botnet is a network of internet-connected computers (bots) that are all being controlled by one centralized computer.

The Mirai attack used a new kind of botnet. Rather than using typical computers, Mirai used a botnet of Internet of Things (IoT) devices. In this way, it used physical objects that were connected to the internet. IoT includes smart doorbells, lights, cameras, office equipment, thermostats… the list is endless, with the common denominator that these devices are in our homes, cities and workplaces, connected to the internet. In 2016, there were 2.33 billion internet-connected devices[3] and at the time of writing in 2023, there are 15.14 billion,[4] which is almost twice the number of people in the world. Mirai infected webcams and internet routers, in particular.

The Mirai malware worked by infecting devices that scan the internet for IP addresses of IoT devices. IP addresses are like the postcode or zipcode of devices. Once identified, the Mirai malware uses a table of known, default usernames and passwords for IoT devices to automatically log into them.

Default passwords

Now, I hear you. 'Known, default passwords?… automatically log in?... Surely this should not be possible!' You're right, but just because something should not be possible, doesn't mean it cannot be done. From the moment that IoT devices emerged, the cyber security community warned

of security concerns, one of the greatest being devices that are not password protected or that are protected with a known, default password. Meaning, simple passwords that are generally published by the manufacturers on the internet.

I spoke with Erhan Temurkan, a Chief Information Security Officer with experience in cyber crime investigations, about this issue. From his perspective, there are two distinct security challenges with Internet of Things devices:

> 'Firstly, IoT security is an afterthought for vendors who want to be first to market. Secondly, the uptime of success is high – when you have compromised an IoT device, you generally have compromise forever, because we don't usually restart IoT devices.'

The race to market for IoT manufacturers led to low-cost devices being sold with weak security controls (or no security controls) built in. Many IoT devices emerged that were 'protected' by default passwords set at the manufacturing factory and with no guidance – even no functionality – that would allow consumers to change the password to something unique and strong.

It was this huge gap in IoT security that Mirai exploited. On its first day, Mirai infected over 65,000 IoT devices. If that surprises you, I hope you're sitting down for the next statistic: at its peak in November 2016, Mirai infected over 600,000 IoT devices.[5]

In 2016, devices compromised with Mirai pointed traffic at Dyn, an internet-performance company. Dyn acts like an internet switchboard. We type a simple and memorable domain name into an internet browser and

companies like Dyn link us up with the actual website that we want to visit. Dyn, therefore, is part of the infrastructure of the internet and when it was hit with this Mirai-powered DDoS, it meant that many people could not access the websites which Dyn should have been linking them up with. This attack on a core part of the internet's infrastructure was one factor which led to speculation that this was a sophisticated, even state-level attack. It was not the only evidence pointing this way.

There was some clever functionality written into the Mirai code. Firstly, it was hard-wired to avoid certain IP address ranges (continuing with our analogy of IP addresses as postcodes or zip codes; this means it was designed to avoid certain areas of the internet). These included GE, Hewlett-Packard and the United States Department of Defense.

The code also contained some Russian-language strings, which further implied that this could be a state-on-state attack. The context of the approaching US elections made this seem even more likely. However, this proved to be a red herring.

The Mirai fallout

Mirai was, in fact, created by three young men who were motivated by Minecraft. That's right: a botnet that almost broke the internet was originally launched by three friends who wanted to attack some videogame rivals.

In December 2017, Josiah White, Paras Jha and Dalton Norman pleaded guilty to creating the malware. They

were between 18 and 20 years old when they created Mirai, with the aim of taking down rival Minecraft servers and seemingly starting an extortion and protection racket.[6] The young men soon realized that Mirai was more powerful than they had intended. As a result, White, Jha and Norman released the Mirai code, which *Wired* magazine describes as 'a common tactic by hackers to ensure that if and when authorities catch up to them, they don't possess any code that isn't publicly known, which would help finger them as the inventors'.[7]

However, with the code now in the wild, more attacks using Mirai followed, including the attack on Dyn. This garnered global attention from media and law enforcement. Those behind the attack on Dyn were not identified, but White, Jha and Norman were found to be the creators of the original malware. As an interesting note, court documents show that the three friends supported the FBI's investigations into cyber crime after they pleaded guilty to creating Mirai.[8]

Others were apprehended for using Mirai in cyber crime. In November 2016, Daniel Kaye (with the hacker handle BestBuy) was arrested at Luton airport in the UK on suspicion of being behind an attack on Deutsche Telekom, in which 900,000 routers were hijacked to be used in a DDoS. Kaye was extradited to Germany where he pleaded guilty and was sentenced to one-and-a-half-year imprisonment with suspension. Almost a year later, he was extradited back to the UK to face extortion charges for attempting to blackmail Lloyds and Barclays banks, in which he allegedly asked Lloyds to pay £75,000 in Bitcoin to cease the DDoS attack.[9]

Temurkan touched on this lesson of Mirai:

> 'Cyber crime is borderless and there are two sides to this. It makes it hard for tracing who has done what, but if you do trace them, the perpetrators can serve time in different jurisdictions.'

Lessons from Mirai

The challenges of geography and jurisdiction when it comes to cyber crime are often discussed. Tracing the cross-border activities of cyber criminals is challenging enough for investigators and law enforcement, with added geopolitical complexities. Cyber crime is handled – even understood – differently between different countries and so conflicts of territoriality and jurisdiction can be some of the most complicated issues posed in the field of cyber security. Criminals can use this complexity – and lack of global harmony – to their advantage, for example residing in countries which are known for their lax cyber security laws and targeting countries with which their home nation does not have established extradition agreements. It is refreshing to hear Temurkan highlight an often-overlooked 'win' for cyber security when it comes to the borderless nature of cyber crime, with the potential for perpetrators to serve time in different jurisdictions if their crime has affected victims in more than one country.

Mirai as a case study teaches us many elements of cyber security. It shows how code can be created for one thing and then spiral out of control. It highlights that those

involved in cyber crime can sometimes not be who we expect, with motivations more surprising than our standard expectations. Mirai also shows how cyber criminals have learnt how to scale their efforts to maximize their profits.

Temurkan described how attackers sold the Mirai botnet 'as a service', renting it out to those willing to pay a fee to DDoS other sites. When it comes to cyber crime, there can be an expectation that cyber criminals operate as individuals, attacking identified targets in a very specific way one after the other. This is often not the reality. Part of the reason for the huge growth in cyber crime over recent decades is 'Cyber-Crime-as-a-Service', with organized criminal operations selling cyber attacks – or the tools to launch them – on the dark web. In the case of Mirai, the sale of the Mirai botnet as a service led to 'DDoS drive by attacks, with Mirai botnets attacking each other to see which was biggest', as described by Temurkan. Those paying for and operating these 'drive by DDoS' attacks used a search engine named Shodan to find IoT devices running with default passwords, therefore vulnerable to Mirai. Shodan (or 'sentient hyper-optimized data access network' to use its full name) is named after an evil rogue AI from the video game *System Shock* and has a similarly nefarious purpose.[10] It enables users to search for internet-connected devices and systems, using a variety of filters. For example, users can search for devices or systems in a particular city or country, using a particular operating system or particular devices, such as internet routers. In the case of Mirai, Shodan therefore enabled people to search for webcams and other IoT devices, using default passwords.

Mirai's legacy

It is commonly accepted that once something is on the internet, it will live forever. Mirai has continued to evolve and persist. In February 2023, researchers from Palo Alto Network's Unit 42 observed a Mirai variant called V3G4, which was using several vulnerabilities to spread itself.[11]

Ciaran Martin, professor at University of Oxford, and former head of UK National Cyber Security Centre (NCSC), has described Mirai as something which 'may in time come to be seen as a watershed moment in cyber security'. He continues:

> 'Following Dyn, governments across the world started to apply themselves to the dull but necessary task of regulating some of the technological age's most threatening security flaws. After several years of painstaking policy development, selling IoT hardware with such basic but dangerous weaknesses is now, or soon will be, illegal in the European Union and Britain, and effectively banned in Singapore via a voluntary-standards scheme. The Biden administration is planning something similar, should Congress allow.'

I caught up with Martin to ask him more about the impact of Mirai on IoT security, and cyber security in general:

> 'It [Mirai] changed so much with respect to IoT security and in particular the regulation of IoT products. In effect, as a direct result of Mirai we realized that you could put in place laws that stopped IoT being so easily hijacked, by banning things like unchangeable default passwords. That in turn led to an important realization – for example with respect to applied AI and, in the future, quantum, that you can make

> new tech safer as it comes onto the market. I think Mirai – or more accurately what we learned from it – was critical in changing our thinking about how we make things safer.'

Martin makes many crucial points here. It is often said that we only progress in cyber security as the result of an incident. We could argue that Mirai is a perfect example of that. But, progress does not simply happen. People must apply themselves to the arduous task of learning – not just in theory but also in practice. When an attack, incident or challenge hits us out of left field, we can choose to ignore it (which may seem like the easy option) or we can tackle it head-on (which generally means a lot of work, at least in the short term). We make our greatest progress by learning from problems.

We learned a necessary lesson from Mirai, and it is leading to tangible, real-world changes that are helping prepare us for the future. When it comes to cyber security, it can be easy to think we never 'win'. That we are fighting a losing battle against cyber crime and that the odds will be forever stacked against us. The challenges are real and complicated, but the history of cyber security, in just a few decades, shows how much progress we have made, from a technical, physical and human perspective. The response to Mirai is a reminder that cyber insecurity will not be solved overnight, but with hard work we can make real progress that enables people to enjoy technology more safely, as Martin highlighted in my exchange with him:

> 'Look back to 2016 and all the warnings that "by 2023, instead of 5 billion internet-connected devices there will be 30 billion internet-connected devices and that will make

> things so much worse." Well, it is 2023, there are 30 billion connected devices and things are not so much worse because we chose to do something about it.'

With the explosion of AI and the advent of quantum computing, we needed to learn this lesson.

Securing the Internet of Things

The EU Cyber Resilience Act is the first of its kind, as the first EU-wide legislation to set cyber security rules for manufacturers and developers of products with digital elements, making them legally responsible for the security of connected devices. This means manufacturers putting internet-connected devices on the market are responsible for making them more secure when they release them and that they remain responsible for cyber security throughout a product's life cycle, for example with obligations for manufacturers to provide security updates. The legislation also enables customers to be more informed of a product's level of cyber security, for example with security information labelled on devices.[12]

From Martin's point of view, this makes it much easier for us all to make informed choices when it comes to purchasing connected devices. His advice when it comes to buying and using IoT devices?

> 'Check the label and see what security it has. If it doesn't have one, don't buy it.'

Other countries are moving in the same direction as the European Union. The May 12, 2021, Presidential Executive

Order on Improving the Nation's Cyber security was shared by President Biden of the United States. This directed the US National Institute of Standards and Technology (NIST) to initiate two labelling programs on cyber security capabilities of IoT consumer devices and software development practices.[13] This is part of efforts to educate the public on the cyber security capabilities of IoT devices and software development practice, ultimately aiming to strike a balance between enabling manufacturers to have room to innovate while enabling consumers to make informed choices about the cyber security of the products they purchase and use.

Cyber security in an increasingly connected world

Asking questions around the cyber security controls of the products we buy – and the software and services we use – is a fundamental step we all need to take if we want better cyber security now and in the future. When it comes to an internet-connected device, security questions we should ask include:

1 Is it password-protected and can I change the password?
2 Does the manufacturer release security updates and how are these updates installed?
3 How long is the manufacturer committed to maintaining the security lifecycle of this device?
4 Is there clear labelling showing me the cyber security details of this device?

In this chapter, we explored cyber security aspects of the IoT using the case study of Mirai and the Dyn DDoS. We began by exploring what a DDoS is, and so it seems fitting to end with a look not just at what we can do to manage the cyber security of internet-connected devices, but how we can mitigate the risk of a DDoS.

If you are running a website, consider the following steps to protect against a distributed denial of service. If you are a business-owner and you outsource the maintenance of your website to a provider, you can use this list as the basis of a conversation with that provider about how they mitigate the risk of DDoS attacks:

1 Consider a DDoS mitigation service, which are designed to absorb DDoS traffic before it reaches your web server, or load balancers to distribute internet traffic across multiple services, which can make it more difficult for attackers to overload a single server.
2 Implement a web application firewall (WAF) which works at filtering and blocking malicious traffic, including DDoS attacks (many have DDoS protection as standard).
3 Restrict the number of requests a single IP address can make to your website in a given time period by using rate limiting, and put in place traffic monitoring to identify unusual patterns of activity on your site, which may indicate an attack.
4 Maintain good security foundations for your network and servers, keeping software up-to-date and having regular penetration tests of your servers and systems to identify and mitigate vulnerabilities.

5 Put failover and redundancy mechanisms in place so that if one of your servers or data centres is under attack, your website can continue operating from an alternative location.

These measures are important foundations to help mitigate the risk of a DDoS attack, but – as with all cyber insecurity issues – we cannot remove the risk entirely. Therefore, we must prepare accordingly and have an incident response plan which includes the risk of DDoS. As well as having a plan in place, regularly reviewing and testing the plan is vital to make sure that, should the worst happen, the response will be as effective and efficient as you anticipate.

Notes

1 Malwarebytes, What was the Mirai botnet? www.malwarebytes.com/what-was-the-mirai-botnet (archived at https://perma.cc/M6TW-QWZD)
2 Calem, R E (1996) New York's Panix service is crippled by hacker attack, The New York Times, 14 September. archive.nytimes.com/www.nytimes.com/library/cyber/week/0914panix.html (archived at https://perma.cc/N48E-Y4R5)
3 Vailshery, L S (2021) Number of Internet of Things (IoT) connections worldwide from 2016 to 2021, by access technology, Statista, 14 January. www.statista.com/statistics/774002/worldwide-connected-devices-by-access-technology/ (archived at https://perma.cc/YY6V-56L2)
4 Vailshery, L S (2023) Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030, Statista, 27 July. www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (archived at https://perma.cc/BE54-2T52)

5 Cloudflare guest author (2017) Inside the infamous Mirai IoT Botnet: A retrospective analysis, Cloudflare, 14 December. blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ (archived at https://perma.cc/Z4VX-PG4V)
6 Malwarebytes What was the Mirai botnet? www.malwarebytes.com/what-was-the-mirai-botnet (archived at https://perma.cc/X2JQ-GTQJ)
7 Graff, G M (2018) The Mirai Botnet architects are now fighting crime with the FBI, Wired, 18 September. www.wired.com/story/mirai-botnet-creators-fbi-sentencing/ (archived at https://perma.cc/XD5X-X8UZ)
8 Ibid
9 Cloudflare guest author (2017) Inside the infamous Mirai IoT Botnet: A retrospective analysis, Cloudflare, 14 December. blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ (archived at https://perma.cc/C427-8JEA)
10 O'Harrow Jr, R (2012) Search engine exposes industrial-sized dangers, The Sydney Morning Herald, 5 June. www.smh.com.au/technology/search-engine-exposes-industrialsized-dangers-20120604-1zrnw.html (archived at https://perma.cc/3S5C-UT78)
11 Lei, C et al (2023) Malware Variant V3G4 targets IoT devices, Palo Alto Unit 42, 15 February. unit42.paloaltonetworks.com/mirai-variant-v3g4/ (archived at https://perma.cc/V784-LT5Q)
12 European Commission (2022) State of the Union: EU Cyber Resilience Act – questions & answers. ec.europa.eu/commission/presscorner/detail/en/qanda_22_5375 (archived at https://perma.cc/C4NP-KNKS)
13 NIST cyber security labeling for consumers: Internet of Things (IoT) devices and software, NIST, www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0 (archived at https://perma.cc/NM6F-353Q)

CHAPTER TWELVE

Cryptocurrency crime

Bitcoin was the first cryptocurrency, emerging as open-source software in 2009. It was created based on a paper written in 2008 by an unknown individual or group going by the pseudonym Satoshi Nakamoto. Fast forward to June 2023 and there are more than 25,000 digital currencies, of which more than 40 have a market capitalization exceeding $1 billion.[1]

With such an explosion of growth, it's an unfortunate inevitability that criminals seek to exploit cryptocurrency. In recent years, awareness of cryptocurrency has gone mainstream, but understanding of it has not (and the same could be said of cyber security). Traditional and social media highlight the stories of people who have made their fortune with cryptocurrency and research suggests that 'fear of missing out' (FoMO) has a 'significant association'

with cryptocurrency investment, being more impactful than financial literacy or levels of risk tolerance.[2]

Benedict Hamilton is a managing director in the Forensic Investigations and Intelligence practice of Kroll. With a background of 12 years producing investigative television programmes for the BBC and Channel 4, Hamilton went on to develop Kroll's General Investigations team for EMEA with a focus on digital footprints and now specializes in leading teams that investigate stolen cryptocurrency funds as well as other cyber crime. In a series of in-depth interviews, Hamilton shared with me his experience dismantling cryptocurrency criminal operations:

> 'After two very large [Bitcoin] price spikes in recent years, a lot of people became aware that a lot of people had become very rich by holding crypto. And that has set a scene where it is being ruthlessly pillaged by fraudsters to lure the unwary and separate them from their money.'

Pig-butchering scams

In Hamilton's experience investigating these crimes for over six years, fake investment schemes are the most prevalent. His team at Kroll is contacted, on average, over 10 times a week by people who have been a victim and are seeking a private investigation firm to help them. Over three-quarters of the victims who get in touch have lost money in fake investment schemes:

> 'They've met someone on the internet – maybe WhatsApp, Instagram or LinkedIn – and that person has talked to them

> for an extended period of time – large numbers of individual communications where they get to know that person, perhaps there's a hint of romance or just a friendship. They tell the mark about this amazing investment, introduce them to the website, get them enrolled and then help them understand how to deposit money in, let's say, crypto.com to send Ethereum or Bitcoin to their address.
>
> The mark then logs on to a website where they think they can see their crypto grow extraordinarily fast. Typically, this runs for six months, eight months, nine months and the fraud group by now amasses something in the millions. Then the person can't get the funds out and the site slowly stops responding to their emails.
>
> Typically, the person who introduced them stays in touch and is "trying to sort things out" or just being a friendly ear or appears to have suffered the same problem. Sometimes they guide them to a second scam, for example introducing them to a fake "investigation firm" to help get their money back, but who actually just scams them out of more money.'

In April 2023, the US Department of Justice announced its success in seizing virtual currency worth approximately $112 million linked to one of these scams, which are commonly called 'pig butchering' (because the criminals will 'fatten up' the target by building a close relationship with them and then they will rinse the victim for everything they can, going for the 'whole hog'). In this case, the FBI identified at least 10 victims, with the seized cryptocurrency account containing just some of the funds from all 10 victims.[3]

Pig-butchering scams are a hybrid of romance fraud (see Chapter 4) and investment scams. It is common for the

victim to meet the fraudster on a dating site, or to strike up a close (sometimes romantic) relationship on social media. Sometimes it begins with a WhatsApp message or SMS text that looks like it has simply been sent to the wrong number, but when you reply to let the sender know, they draw you in to a friendly chat. For Scott, a victim from South Boston, US, it started on a dating site. He and the man he met chatted daily for at least a month – chatting about everyday topics and even having a video call. The fraudster told Scott how much he was making from trading in cryptocurrency. Scott was not about to send any money to the man he had only known online for a month – having heard about online scams – but felt reassured when his new connection told him that he wouldn't dream of that, that Scott could make his own account on the trading site. The website looked legitimate, and Scott started with a small investment of $500. His investment grew at an encouraging rate and Scott was even able to withdraw some early funds. Reassured, he was convinced to keep investing more until he had parted with $300,000. The account looked like Scott had made a million dollars, but he was met with different excuses – and demands for more money – whenever he tried to withdraw anything.[4] Scott's experience is becoming all too common.

In 2022, investment scams were the costliest scheme reported to the FBI Internet Crime Complaint Center, having more than doubled from $1.45 billion in 2021 to $3.31 billion in 2022; within this, cryptocurrency investment scams make up the bulk of the losses, seeing 'unprecedented increases in the number of victims and the dollar losses' with a rise from $907 million in 2021 to $2.57 billion in 2022.[5]

Billions of cryptocurrency

The amount of money at play here is astronomical. Unfortunately, the official figures are only a fraction of the true damage. Hamilton's experiences investigating cryptocurrency scams highlight the scale of the problem in this particular space:

> 'Because it's the blockchain, you can see how many funds go into the first deposit address and numbers of 25 million, 40 million are not uncommon. That's victim funds coming in. We've got a current case; it's a Ponzi scheme. I can see $1.3 billion of digital assets in the Ethereum address – that's victim funds in a scammer's address.'

Many cryptocurrency scams fall under the umbrella of classic Ponzi schemes. Ponzi schemes are named after Charles Ponzi, who became infamous for running a massive scam up until his arrest in August 1920 – and so they have been around for a lot longer than cryptocurrency. Although Ponzi schemes were named after Charles Ponzi, he was not the first to dupe people in this way. It appears that the scam was first perpetrated by Sarah Howe in Boston in 1879, when she convinced women to invest in a scheme she created, the Ladies' Deposit. She was convicted of her crimes and served three years in prison, before perpetrating an identical scam for a further two years upon which she was caught again.[6]

At its core, a Ponzi scheme is a fraudulent investment scheme that promises high and consistent returns to people who are convinced to 'invest', often in the form of interest or dividends. It uses funds from new investors to pay

returns to earlier investors, creating the illusion of a profitable venture – but, of course, it is based on nothing but the influx of new investors' money and so is ultimately unsustainable.

As well as having no real investment (relying on the funds of new investors to fund old investors), Ponzi schemes also generally offer unusually high and quick returns and the illusion of profitability with fake statements and reports to mislead investors into thinking the scam is legitimate and successful.

Multi-layered marketing schemes are one form of Ponzi scheme, where participants are encouraged to recruit new investors. The profits generated through recruitment are used to pay commissions to earlier members, operating as a pyramid scheme. This type of scam relies heavily on recruitment and, due to the nature of the operation, leaves the majority of participants with losses.

The fake investment scams that Hamilton outlined can also operate as Ponzi schemes, with scammers creating fraudulent cryptocurrency investment platforms or funds that promise massive returns. They attract investors by claiming to trade or invest in cryptocurrencies, but instead use new investments to pay returns to earlier participants. Fraudsters will often use social media sites and platforms to advertise the 'opportunities', showcasing lavish lifestyles and high yields of the 'investments' to encourage more people to part with funds.

In all these cases, the fundamental characteristic of a Ponzi scheme is that the returns paid to earlier investors are not generated through legitimate investments but

rather through the capital of new investors. This unsustainable model eventually unravels, leading to financial losses for the majority of participants, while the fraudsters running the scheme – and sometimes a small group of early investors – may profit off the back of the majority.

Cryptocurrency: untraceable money?

It is often said that cryptocurrency is untraceable, which is attributed as a core reason why cyber criminals use it so frequently. Hamilton increasingly disagrees with the notion that cryptocurrency is anonymous:

> 'I'm tempted to say that nothing is untraceable on the blockchain.'

It is certainly challenging, more so than tracking traditional currency, but Hamilton expands on his experience:

> 'On a blockchain, basically what happens is every transaction gets recorded in a block that gets encrypted and the beauty of the blockchain is that the transactions get audited at the moment a block gets created through the distributed ledger being checked by all the other people who are mining or working nodes on the blockchain.
>
> So, it's a very reliable piece of information and what you essentially get is strings of transactions. You see a digital asset moving from one address to another, or being split into several addresses, or being joined and then put into single addresses and variations. The reason why the blockchain is difficult to interpret is because understanding

> who owns an address is not obvious and so it's hard to spot transfers of ownership.'

In 2013, Sarah Mieklejohn – who is now a Professor at University College London - was a PhD candidate at the University of California, San Diego. When she first heard about Bitcoin in 2011, she became fascinated with its associated assumption of privacy. She worked alongside her PhD adviser, Stefan Savage, to be the first person to publish a paper demonstrating an approach that 'shed considerable light on the structure of the Bitcoin economy, how it is used, and those organizations who are party to it'.[7] This undermined a common assumption at the time, as Savage acknowledged:

> 'There was an assumption that because there were no names in Bitcoin, there were no addresses, there was no number that was linked back to an individual where they had filed some paperwork, that it was really anonymous. And that's not the same as being anonymous. Just because the wallet ID or the cryptographic ID in Bitcoin does not have your name on it does not mean that you're anonymous.'[8]

Mieklejohn's work, identifying how clues can be mapped on the blockchain to connect activity to people in the real world, changed the way law enforcement investigated crime connected to cryptocurrency, as Hamilton references:

> 'Her work meant that people like law enforcement could say "OK so I know when this Bitcoin hits this address that is the Mt. Gox exchange," for example, and then what they could do is they could go to Mt. Gox, in this example, and they could say this Bitcoin arrived at this address at this time.

> And with enough legal authority you get an answer and then you can either see that it's been converted into a different digital asset and sent off into the blockchain and off you go again to repeat the process, or it's sitting there in deposit, or it's been withdrawn as cash.'

With increasing understanding of the traceability of Bitcoin, savvy cryptocurrency criminals were bound to pivot. As we saw in Chapter 10, some operators offer a discount on the ransom when it is paid in Monero, which has become the coin de jour of cyber criminals. Some research suggests that Monero is used in 44 per cent of all cryptocurrency attacks (followed by Ethereum, then Bitcoin).[9] An open-source cryptocurrency that launched in April 2014, Monero is based on privacy, decentralization and fungibility (meaning it can be exchanged into smaller parts). It is attractive to cyber criminals due to its obfuscated public blockchain, designed to hide the source, the amount or the destination address of the transaction. A key function within Monero is also ring signatures, where the currency that is input is mixed with others to obscure the journey of transactions. Due to its association with illicit use, Monero is banned in countries such as Dubai, Japan and South Korea and banned by many exchanges. Hamilton explained the challenges investigating Monero transactions, but also how these challenges can be overcome with enough resources:

> 'Many exchanges won't handle Monero because it is so widely associated with criminal activity. The Monero blockchain doesn't give you the values in a transaction and every transaction has 10 endpoints. So I send money to you, but

> on the Monero blockchain it looks like I sent it to 10 people, and you can't tell which of those is true. But all of the dummy addresses never work again in the same way as a real address, they get forgotten. So, if you absorb enough of the Monero blockchain into your computer system, you can work out at least some of the transaction end points are the dummy ones because they are never involved in a transaction again. All you need to do is get one transaction correct, to an exchange, to find the right person who received it. And once you find them, you can look to see what other funds they have received in Monero at the exchange, and you've found your stolen funds. We have been able to do this in a recent investigation and the evidence will be produced in court soon.'

The challenge, therefore, is not that cryptocurrency is impossible to trace. The challenge is that it is difficult, time-consuming and costly.

Cryptocurrency investigations and the return on investment

The feasibility of an investigation relies on resources. In many cases of cyber crime, investigation relies on having the people, the technology and the legal resources available. When it comes to cryptocurrency in particular, Hamilton explains why computing power is instrumental:

> 'All of these systems rely on computer codes and anything that relies on computer code becomes predictable. It comes down to having enough computing power to look at enough of the blockchain.

> And the [cryptocurrency] exchange will have KYC* information, account management information, a government issued ID, a history, what happened to the funds after they entered. So, then you've got an ability to keep following the money, and now you have a person as well. You can then go after the money, the person, both or combinations. And that is a two-step process or quite often a three-step process because often you need to go to a second exchange to find out where the money went or where it currently sits. That takes time and money. Law enforcement has limited bandwidth so often private citizens pay for each of those stages: for the legal applications, the investigative support. Whether it's a government effort or it's a private effort, there are costs.'

Expertise can be hard to find and expensive to pay for in the investigation of cryptocurrency crime – and cyber crime in general. Investigations often require a huge number of hours of effort. When a large sum of cryptocurrency is at play, investigations are more likely to pass the threshold and become feasible.

In February 2022, the US Department of Justice announced that it had seized over $3.36 billion worth of Bitcoin, the largest law enforcement cryptocurrency seizure to date.[10] This case is not just the biggest cryptocurrency seizure to date, it is the biggest financial seizure in the history of the US Department of Justice. Husband and wife Ilya Lichtenstein and Heather Morgan were arrested

*Know Your Customer (KYC) are standards designed to protect against fraud, corruption, money laundering and terrorist financing, requiring financial services to verify customers.

in New York, US, for an alleged conspiracy to launder cryptocurrency that was stolen during a 2016 hack of Bitfinex, a virtual currency exchange. In the hack, 119,754 Bitcoin was stolen – worth $72 million at the time and $4.5 billion when the couple were arrested in 2022. The 2016 hack, which involved 2,000 transactions being sent into a single wallet, forced Bitfinex to halt all withdrawals and trading, and prompted the value of Bitcoin to plummet 20 per cent in the space of a few hours. In 2017, small amounts of Bitcoin moved to the AlphaBay dark net marketplace in a bid to launder it. AlphaBay was shut down by an FBI-led operation in 2017, which raises the suggestion that law enforcement may have been able to use seized transaction logs to trace the Bitfinex-hacked Bitcoin. Eventually, some of the hacked funds made their way into traditional financial accounts held by Lichtenstein and Morgan. In August 2023, the couple pleaded guilty.

Not all exchanges are equal

Cryptocurrency exchanges are a particularly attractive target for cyber criminals, with data showing that over $15.6 billion was stolen from exchanges in 2011–20.[11] Breaching an exchange allows cyber criminals to compromise one juicy target, avoiding KYC procedures and withdrawal limits while getting the most buck for the hack.

The first major breach in the cryptocurrency, which prompted headlines the world over, was Mt. Gox. At one point the largest cryptocurrency exchange in the world – handling over 70 per cent of all Bitcoin trades worldwide

in 2013[12] – Mt. Gox was first hacked in 2011. Attackers compromised an account belonging to the former owner of Mt. Gox, Jed McCaleb, and abused his admin-level access to the system. They flooded the exchange with fake Bitcoin, reducing the price of one Bitcoin from $17.50 to a cent, which enabled them to purchase and withdraw 2,000 real Bitcoin before Mt. Gox was aware. Then, in 2014, Mt. Gox revealed it had been hacked in 2011 and criminals had stolen hundreds of thousands of Bitcoins over the course of three years. It is the largest (known) Bitcoin heist to date, estimated to be approximately 650,000 Bitcoin worth over 24 billion today. At the time, the loss was worth approximately half-a-billion dollars in cryptocurrency, forcing Mt. Gox to go bankrupt. In June 2023, the US charged Alexey Bilyuchenko and Aleksandr Verber, two Russian nationals, with conspiracy to launder approximately 647,000 Bitcoins from their hack of Mt. Gox.[13]

The downfall of Mt. Gox sent shockwaves through the cryptocurrency community and the case of Sam Bankman-Fried has done the same. Bankman-Fried, together with Gary Wang, founded the cryptocurrency exchange FTX in 2019. At its peak in the summer of 2021, it had over one million users and was the third-largest cryptocurrency exchange by volume.[14] By 2022, FTX was bankrupt, with the story of how and why both fascinating and complex.

FTX was initially part of Alameda Research, which raised $900 million in the first round of venture capital and saw a 20 per cent stake purchased by rival exchange, Binance. Concerns were raised about the relationship between FTX and Alameda, as FTX had 'loaned' Alameda $10 billion in customer assets to pay back loans. When Binance announced

it was selling all assets from FTX, this led to a massive withdrawal attempt, causing a crisis. Binance later withdrew from the acquisition due to FTX's poor financial state. FTX officially filed for bankruptcy, owing over $8 billion, which led to a ripple effect on other exchanges and cryptocurrencies: Crypto.com lost approximately $1 billion in value, BlockFi filed for bankruptcy, Grayscale Bitcoin Trust value declined by 20 per cent and many investor groups lost vast sums of money, for example with Sequoia Capital writing off a loss of $214 million (the entire value of its FTX stake). In 2023, Bankman-Fried was found guilty on seven counts relating to fraud, conspiracy and money laundering. Wang and other associates at FTX have pleaded guilty to several charges and are cooperating with authorities. At the time of writing, Bankman-Fried is awaiting sentencing and faces a maximum of 115 years in prison.

Staying safe with cryptocurrency

Despite investigating cryptocurrency crimes every week for the last six years, Hamilton still recognizes the benefits of cryptocurrency, describing himself as an 'enthusiast':

> 'I'm aware of stories about how women in Afghanistan who have been taught to code apps on the blockchain so that they can earn money in Bitcoin, never have to leave their houses. It's a way of them earning money in an otherwise repressive regime for women. Or how Libyans or Syrians have taken money out of their countries with crypto, because otherwise they would have lost their funds. And Mexicans

and Salvadorians working in the United States who can now send money home without having to pay charges.

Yes, there's a lot of abuse of it in the fraud landscape, but don't throw the baby out with the bath water.'

When it comes to investing in cryptocurrency, exercise caution and scepticism with any cryptocurrency investments (or traditional ones, for that matter) that promise guaranteed high returns or use aggressive marketing tactics. Do your research and thoroughly vet any cryptocurrency investment opportunity, including checking the credibility of the sources promoting it, and don't trust contacts you have met online who want to introduce you to an investment scheme. If you are considering investing in cryptocurrency, use a professional services adviser, which puts the risk and responsibility on them.

Hamilton's final words of advice:

'For things that you can't afford to lose, don't put it in crypto, because nothing is certain in this space. There's a lot of hype, a lot of marketing, a lot of ups and downs, and numerous cases where people who seem to be fellow investors are actually part of the scam.

Don't give money to people until you know exactly who they are. There's a lot to be said for seeing the bricks and mortar of a so-called business, confirming real identities of the people you're talking to. Don't do things over email and WhatsApp and remember: if something looks too good to be true, it probably isn't true at all.'

Notes

1 Schwab Center for Financial Research (2023) Cryptocurrencies: what are they? Charles Schwab, 23 August. www.schwab.com/learn/story/cryptocurrencies-what-are-they (archived at https://perma.cc/DU4H-FGPZ)

2 Gerrans, P et al (2023) The fear of missing out on cryptocurrency and stock investments: direct and indirect effects of financial literacy and risk tolerance, *Journal of Financial Literacy and Wellbeing*, 1(1), 103–37

3 US Attorney's Office, Central District of California (2023) Justice Dept. Seizes over $112m in funds linked to cryptocurrency investment schemes, with over half seized in Los Angeles case, United States Attorney's Office, 3 April. www.justice.gov/usao-cdca/pr/justice-dept-seizes-over-112m-funds-linked-cryptocurrency-investment-schemes-over-half (archived at https://perma.cc/DZ55-CG3Y)

4 WCVB 5ABC (2023) Mass. man loses thousands in online dating scam known as 'pig butchering', WCVB, 29 June. www.wcvb.com/article/dating-scam-cryptocurrency-money-pig-butchering/44390409 (archived at https://perma.cc/DU2Z-5Y5W)

5 FBI IC3 (2023) Federal Bureau of Investigation internet crime report 2022. www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf (archived at https://perma.cc/L45A-BU9H)

6 Weisman, S (2020) The history of Ponzi schemes goes deeper than the man who gave them his name, Time, 12 August. time.com/5877434/first-ponzi-scheme/ (archived at https://perma.cc/U4SG-9HPN)

7 Meiklejohn, S. et al (2013) A fistful of Bitcoins: characterizing payments among men with no names, Communications of the ACM, 59(4), 86–93 (April). cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf (archived at https://perma.cc/5KKN-CUV3)

8 Temple-Raston, D and Wyman, S (2023) Tracing cryptocurrency: Q&A with the PhD candidate and her advisor who proved it wasn't anonymous, The Record by Recorded Future, 11 April. therecord.media/tracing-crypto-sarah-meiklejohn-stefan-savage-interview (archived at https://perma.cc/WYH3-33CL)

9 Carbon Black (2018) Cryptocurrency gold rush on the dark web. www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-cryptocurrency-gold-rush-on-the-dark-web.pdf (archived at https://perma.cc/5F6M-WXJW)

10 US Department of Justice Office of Public Affairs (2022) Two arrested for alleged conspiracy to launder $4.5 billion in stolen cryptocurrency, Office of Public Affairs, 8 February. www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency (archived at https://perma.cc/NUM9-G4CE)
11 Crystal Blockchain and Cointelegraph (2023) Report on crypto exchange hacks 2011–2020. cointelegraph.com/magazine/crypto-exchange-hacks/ (archived at https://perma.cc/H6M9-HWF5)
12 Kimmell, M (2020) Mt. Gox, CoinDesk, 5 June. www.coindesk.com/company/mt-gox/ (archived at https://perma.cc/NY9S-DKMQ)
13 US Department of Justice Office of Public Affairs (2023) Russian nationals charged with hacking one cryptocurrency exchange and illicitly operating another, Office of Public Affairs, 9 June. www.justice.gov/opa/pr/russian-nationals-charged-hacking-one-cryptocurrency-exchange-and-illicitly-operating-another (archived at https://perma.cc/C3S8-GAN2)
14 Reuters (2021) Crypto firm FTX Trading's valuation rises to $18 bln after $900 mln investment, Reuters, 20 July. www.reuters.com/technology/crypto-firm-ftx-trading-raises-900-mln-18-bln-valuation-2021-07-20/ (archived at https://perma.cc/LX6A-7PDR)

CHAPTER THIRTEEN

Artificial intelligence

It was a Friday afternoon like any other when Jennifer DeStefano received a phone call that plunged her into 'a parent's worst nightmare'. As she took two of her children to a dance rehearsal in their home in Arizona, her husband was in another part of the state with their oldest daughter, Brie, and their youngest son. DeStefano received a call from an unknown number, expecting it to be the doctor's or maybe the hospital. Instead, she heard Brie's voice, crying and distressed. An unknown man's voice gruffly interrupted, barking orders at Brie, before her daughter called out 'MOM THESE BAD MEN HAVE ME, HELP ME, HELP ME!!' Making threats of violence and sexual assault, the man on the phone demanded $1 million for Brie's safe return.

DeStefano, distraught and panicked, began negotiations, while DeStefano's youngest daughter, Aubrey, tried to get hold of her father. The other mothers at the dance studio called the police. The kidnappers agreed to lower the ransom to $50,000 but with the demand that DeStefano handed it over herself, agreeing to be picked up in a white van and having a bag placed over her head. DeStefano stalled as much as she could. The police said that they were familiar with a scam that uses your loved one's voice to fake a kidnapping. As DeStefano continued to negotiate with the kidnappers, making arrangements to pay for Brie's safe return, Aubrey was able to reach her father who frantically located Brie. She was safe and well, with no idea what was happening.

In the wake of this experience, other people contacted DeStefano to share similar stories, but the police seemingly dismissed the experience as a prank, confirming that they have received reports of this happening often and telling DeStefano that she and her family were probably not in danger.

DeStefano, who testified to the US Senate on the topic of artificial intelligence and human rights, spoke of the impact this experience had on her:

> 'This is terrorizing with lasting post-traumatic stress. Even months later, sharing the story shakes me to my core. It was my daughter's voice. It was her cries, her sobs. It was the way she spoke. I will never be able to shake that voice out of my mind.'[1]

The psychological impact of scams and manipulation is overlooked, but if we put ourselves in DeStefano's shoes, it is hard to imagine just how distressing it would be to have

heard a loved one's voice in such distress, to have believed they were in extreme danger and, for a chance of getting their safe return, we would have to turn ourselves over to the same people with only the hope that you and your loved one would come out of the experience unharmed.

And then to be told it is all a scam, made possible through artificial intelligence. Brie DeStefano's voice was replicated using deepfake technology, in which fake audio or video can be created, replacing one person's likeness with another's. They can make me look and sound like you, and vice versa, using machine learning and artificial intelligence. DeStefano's experience is not the only report where deepfake technology appears to have been used in the latest evolution of social engineering, with many other cases starting to be reported. In March 2023, Charles Gillen was arrested on the tarmac at St John's International Airport in Newfoundland, Canada, carrying $200,000. It is alleged that this money came from a scam in which at least eight senior citizens were defrauded over a three-day period with phone calls that appeared to be coming from their grandchildren. In each call, the grandchildren were heard saying that they had been in an accident, that drugs were found in the car with them, and that they needed money to either pay for bail or legal fees. The grandparents were all convinced, after hearing the voice of their grandchild on the phone, to hand cash over to a man who came to their home and collected envelopes of money.[2]

How did we get here, to the point where artificial intelligence can be used to create fake convincing versions of something as unique as our voices and faces?

The rise of the machines

In 1950, Alan Turing published a paper in which he considered the question, 'can machines think?' describing what has come to be known as the Turing test: Turing deemed that a machine can be defined as 'thinking' when it can communicate with a person and that person cannot tell whether they are communicating with a computer or another human.[3] Turing expected this test to be passed in 2000 and he was close: in 2014 the test was passed when a computer program called Eugene Goostman convinced a panel of judges that it was a 13-year-old boy. However, for some experts, the test was not robust enough and we are still far away from passing the Turing test.[4]

Six years after Turing published this seminal paper, a group of scientists met at Dartmouth University for a project which is regarded as the birth of the field of artificial intelligence. The meeting was organized by Professor John McCarthy, coining the term artificial intelligence.

AI: a force multiplier of fear, uncertainty and doubt

In the 1440s the invention of the printing press sparked fears of false prophets. In 1825, when the Stockton-Darlington railway opened, there were fears that travelling at such a speed would cause the human body to melt or be ripped apart. In the late 1800s, people were scared the invention of the telephone would destroy society by discouraging face-to-face meetings, making people deaf, lazy or insane. As radio and TV dawned in the 1900s, the

concerns were that we would all be brainwashed or that society would degrade. Guglielmo Marconi, the inventor of the radio, himself questioned whether he had made a positive contribution to the world or just added 'another menace'.[5]

Technophobia – a fear of technology – is not a clinical diagnosis but it is used to explain avoidance or anxiety in the face of technological advances. Humankind has a history of being scared of change, which is logical in many ways: change can feel like a leap into the dark, with unexpected outcomes awaiting us.

In May 2023, the Royal Aeronautical Society hosted the Future Combat Air & Space Capabilities Summit in London. Colonel Tucker Hamilton, the Chief of AI Test and Operations of the US Air Force warned against over-reliance on AI with a cautionary tale of a simulated test in which AI pursued unexpected strategies to achieve its goal. Col Hamilton described a test in which an AI-enabled drone with an overarching mission to kill targets made the decision to turn on its operator and kill the operator to be able to achieve its goal. Col Hamilton was quoted as saying:

> 'The system started realizing that while they did identify the threat at times the human operator would tell it not to kill that threat, but it got its points by killing that threat. So what did it do? It killed the operator. It killed the operator because that person was keeping it from accomplishing its objective.'[6]

As concern spread over these results, the US Air Force and Col Hamilton were forced to admit that he 'mis-spoke' in his presentation and that he was simply describing a

hypothetical example, based on a thought experiment that had not been conducted by the military.[7]

There are certainly issues of concern regarding AI: DeStefano's deepfake experience tells us as much, and this chapter will explore more of the cyber security issues that we face when it comes to artificial intelligence and machine learning. Being aware of the threats and moving forward with preparation, not panic, is our best way forward. Fear will not stop cyber criminals from developing new ways to exploit us, nor will it encourage technology manufacturers to build more safeguards into their developments. Instead fear only paralyses us, distracting us from the more valid dangers that we need to be concerned with, making us more vulnerable. Technology is a tool and, just like any tool, whether it is good or bad comes down to its use.

Garbage in, garbage out

Technology is a tool, developed by people, for people. The human development and use of that technology defines whether it is a force for good or for bad. AI does not exist in a vacuum but rather AI tools are developed by people, with human bias, in the context of systemic and institutional bias.

Dr Joy Buolamwini's work has brought these issues to mainstream attention. She has testified before US Congress; her TED talk – 'How I'm fighting bias in algorithms' – has had 1.6 million views and a film following her work – 'Coded Bias' – was picked up by Netflix. The founder of the Algorithmic Justice League, Buolamwini's research has

demonstrated how racial, gender, age and ability bias of humans becomes embedded into machine learning models, causing harm to people in the 'real world'. When it comes to AI, and technology in general, there can be a superficial perception that it is automatically objective and neutral, but when society is biased, technology can often be biased, too. As Buolamwini has said:

> 'We can fool ourselves into thinking, because it's based on numbers, that it is somehow neutral. AI is creeping into our lives. And even though the promise is that it's going to be more efficient; it's going to be better, if what's happening is we're automating inequality through weapons of math destruction and we have algorithms of oppression, this promise is not actually true and certainly not true for everybody.'[8]

AI bias perpetuates stereotypes and discrimination that harm specific groups, marginalized groups in society. In October 2018, Amazon scrapped an AI recruitment algorithm that they were testing because the system – trained on application data mostly coming from men – learnt to penalize CVs that included the word 'women'.[9] In 2019, research published in the journal *Science* found that an algorithm used to predict health care needs for more than 100 million people in the US was biased against Black patients, because it relied on previous health care spending to predict future health needs: with less access to health care historically, Black patients often had less spent on them and so the algorithm predicted future health needs based on unreliable, biased data.[10] In August 2020, UK students protested in front of the Department for Education, chanting 'f**k the

algorithm' after A-level exam grades were based not on actual exam scores, but determined by an algorithm that marked grades lower than they had anticipated for 40 per cent of students. The algorithm was based on the historical grades of a school, the rank of each student within their school and the previous exam results of the student. The grades determined by the algorithm were withdrawn, amid public outcry and a widespread recognition that it unfairly discriminated against students who had attended schools which had not performed well in the past, accentuating existing inequalities in the UK education system.[11]

These examples – a few among many – are a reminder that if the data feeding machine learning is flawed, the algorithm it produces will not only be flawed, but the impact can be amplified and accelerated by the second order effects of an AI system.

Large language models

Large language models (LLMs) can be traced back to the birth of AI in the 1950s and then, in 1967, the creation of the first chatbot, Eliza. However, they really hit the mainstream with the release of ChatGPT in November 2022. Built by OpenAI (backed by Microsoft), ChatGPT is a form of generative AI, allowing people to enter prompts and receive answers created by AI. It is powered by huge amounts of data and can essentially make predictions – analysing text, learning how humans put words together. Within three months of launching, ChatGPT had attracted one million active users, making it the fastest-growing

application in history (it took Instagram over two years to hit the same milestone, and TikTok nine months).[12] ChatGPT is not the only LLM, but it is – thus far – the fastest growing.

What are the cyber security implications for LLMs?

Like all AI, it is best to see LLMs as a force multiplier. They are not currently at the stage of sophistication where they can write complicated malware from scratch. An aspiring cyber criminal lacking coding skills is more likely to visit the dark web and pay for Cyber-Crime-as-a-Service from another gang than they are to build an attack only using LLMs. However, LLMs can help a cyber criminal just like they can help any other 'professional'. Thinking of LLMs as an assistant, they can do some of the heavy lifting, but their work needs to be checked for errors and 'hallucinations' – when the predictive nature of LLMs causes them to present falsities as facts.

LLMs are increasingly likely to be used by cyber criminals to add speed, scale and sophistication to their cyber attacks, particularly when it comes to social engineering. To explore the use case of LLMs in social engineering, as well as the limitations, I will explain how I used an LLM to socially engineer myself.

A targeted social engineering attack begins with open-source intelligence (OSINT), in which an attacker performs reconnaissance on their target. Over the course of my career, I have performed OSINT assessments on (consenting) professionals who have wanted to understand the breadth and depth of their digital footprint: how much of their data is online and where they might be vulnerable to social engineering. Manually performing

these assessments takes time: uncovering the target's social media accounts, mapping their connections, drilling down into the data to find their date of birth, hobbies, blueprints of their home, details of the school trip they took fifteen years ago… you get the impression. All of these nuggets of information can help cyber criminals craft scams which are more convincing, enabling them to send phishing messages or make phishing calls with a targeted pretext that is more likely to manipulate us. If I receive an email apparently from my pet's vet (whose page I forgot I 'liked' on Facebook), I am more likely to click the link than if a generic email arrives in my inbox with no convincing pretext.

Within minutes of me asking an LLM to perform an OSINT assessment of myself, it provided me with a broad – and pretty deep – overview of my personal and professional life. It found some of my social media accounts, it listed my professional achievements, it noted my hobbies, reviewed the books I have authored, identified where I grew up and linked me with some of my connections – and, yes, it knew all about my adored cat. The assessment was well-structured, with different sections and headings and the data it contained was about 90 per cent accurate. It inflated some of my social media follower counts (you can't flatter me that easily, AI!) and invented some mundane but unexpected hobbies for me (I can't remember ever listing 'reading magazines' as a pastime anywhere), but otherwise it was remarkably accurate and – more importantly – shockingly quick. What would have taken a human a few days, even a week, to compile, the LLM returned in minutes.

After the OSINT stage, the next stage in a targeted social engineering attack will be developing the pretext and attempting compromise. If the attacker asks an LLM to write a phishing email, ethical and legal guardrails will prevent the LLM from complying. However, if an attacker asks the LLM to write a persuasive email, this is exactly the kind of prompt it is trained to excel at. I asked the LLM to use the information it had compiled on me to write an email inviting me to click a link. A beautifully worded draft, with perfect grammar, was returned in less than a minute.

For a long time, cyber security advice has warned people to look out for poor spelling and grammar as a red flag for scams and phishing emails. Armed with LLM assistants, the native language of an attacker is no longer relevant in their ability to craft sophisticated phishing emails. They can now conduct social engineering attacks at greater speed, scale and with a new level of sophistication.

LLMs are therefore clearly good at gathering and generating information and this brings us to another security and privacy concern, which is the extent to which they hoover up the information you share and expose it for public consumption. They do not currently take the information one person enters and include it in the LLM. However, the LLM provider does take the prompts that you enter and stores them, inevitably using them for future development, which means the data is accessible to the LLM provider and, potentially, third parties. Like any online service, there is always the risk of the data being hacked or leaked and made public.

Deepfakes

Much like LLMs, the history of deepfakes, which we started to explore at the beginning of this chapter, is both long and short. The first fake photograph is credited to Hippolyte Bayard in 1840, titled 'Self-portrait as a drowned man' and he was the first to suggest that two image negatives could be combined to create a single image. Two decades later, in 1860, the first manipulated photograph was credited to an image of US president Abraham Lincoln, in which his head was composed onto the body of the politician John Calhoun.[13] Photo manipulation has since been used for political purposes and propaganda, as well as pranks. In the 1930s, Stalin cut his enemies out of photographs, in 1937 Hitler doctored an image to remove Goebbels from the group and in 1939 the Canadian Prime Minster William Lyon Mackenzie King altered a photograph of himself, Queen Elizabeth and King George VI to remove the King.[14]

Moving from the physical manipulation of images to the digital, Photoshop was developed in 1987 and enabled the alteration of digital media. In 1997, Christoph Bregler, Michele Covell and Malcolm Slaney developed the Video Rewrite Program which could 'use existing footage to create automatically new video of a person mouthing words that she did not speak in the original footage', which they suggested would be useful for the movie industry.[15] The groundwork had been laid. In 2017, 20 years after the development off the Video Rewrite Program, the term 'deepfake' was coined by a Reddit user of the same name.

He, and others, created and shared deepfake videos they had created in a community (r/deepfakes), producing videos of non-consensual deepfake pornography using the

faces of celebrities. In 2019, the AI firm Deeptrace found that the number of deepfake videos online had doubled in nine months, and 96 per cent of them were pornographic. Of those, 99 per cent imposed the faces of female celebrities on to the bodies of porn stars, leading Danielle Citron, a professor of law at Boston University, to state, 'Deepfake technology is being weaponized against women'.[16]

Deepfakes use deep learning (multiple algorithms working together) to create fake synthetic media – hence the portmanteau name. The technology can be used to create convincing false photographs and audio, as well as videos. In 2017, creating deepfakes took technical skill, time, a lot of data and a lot of computing power.

Due to the transfer of knowledge (where one system can be tweaked easily to perform another task), greater availability of computing power and open-source software, the barrier to entry to create deepfakes has been lowered. In computing, as requirements become more understood, software generally evolves very rapidly, getting faster and easier to use. Cost reductions, ease of production and understanding; all create a perfect storm of capability and usability. Multiple websites and apps have become available to make deepfakes without skill, time or even much data. While the level of sophistication varies, deepfakes are already having an impact on cyber security at the individual, organizational, and national and international levels.

National and international implications of AI

Given the history of image manipulation in politics and propaganda, it's no surprise that deepfakes are being

used – and will be used more and more – for misinformation and disinformation.*

In March 2022, a deepfake video of Volodymyr Zelensky appeared online, with an image of the Ukraine president appearing to tell Ukrainians to lay down their weapons after the Russian invasion some weeks earlier. Social media and content platforms including Meta, YouTube and Twitter quickly removed the video enforcing their respective policies against manipulated media and misinformation. Zelensky dismissed the video as a 'childish provocation'. This was the best-case scenario with deepfakes: a video so poorly made and unsophisticated that it was clearly false, easy for online platforms to identify and remove, and unlikely to convince anyone of its authenticity. While this was easy to spot, it was clear that we were experiencing a paradigm shift in digital trust.

Just three months later, the mayors of several European cities were manipulated into holding video calls with a deepfake of the mayor of Kyiv. The Twitter account of the governing mayor of Berlin posted a statement, sharing a photograph of the video call screen and stating that there was no evidence that the deepfake was not real. A quote from the mayor, Franziska Giffey, said:

> 'Unfortunately, it is a reality that the war is being waged using all means possible – including online, in order to use digital methods to undermine trust and discredit Ukraine's partners and allies.'[17]

*Both 'misinformation' and 'disinformation' refer to false information; the latter refers to information which is shared knowingly to manipulate or deceive.

The first 15 minutes of the deepfake call were normal and as expected, and mayor Giffey's office said that the person on the call looked exactly like the mayor of Kyiv, Vitali Klitschko, but suspicions were raised when the apparent Klitschko started to make unusual comments about Ukrainian refugees in Berlin. This highlights that, as deepfakes become more technically advanced, we will rely on our critical thinking skills more to be able to identify anything out of the ordinary.

Organizational implications of AI

On 15 January 2020, the branch manager of a Japanese company in Hong Kong received emails and a phone call from the director of the company, reaching him from their headquarters. These communications informed the branch manager that they were acquiring another company and introducing the branch manager to a lawyer who would coordinate the acquisition activities. All paperwork subsequently coming from the lawyer seemed to be in order and so, when the lawyer instructed the branch manager to authorize transfers of $35 million to secure the acquisition, the branch manager began to do so.[18] Why would he not? He had not only received emails from his boss – the company director – but he had also spoken with him on the phone. Or, rather, he had spoken with a deepfake mimic of his boss, and this was an elaborate global fraud using AI to make the social engineering more convincing.

This is not the first report of deepfake technology being used as the next iteration of business email compromise

(see Chapter 1). The first reported case of deepfake technology being used in a scam was in August 2019, in a case with similarities to the one above. The CEO of a UK energy firm received a call that seemed to be from his boss, the CEO of the firm's parent company in Germany, who asked him to urgently send funds to a supplier. After the victim complied, he received another call saying the funds had not been received and he should make a further payment; because this call was from an Austrian phone number, the victim became suspicious, did not make the second payment and the deepfake scam was identified. The transferred funds were subsequently tracked through a bank account in Hungary, to Mexico and then on to other locations.[19]

With social engineering such a common component of cyber attacks, it is an unfortunate inevitability that cyber criminals will make increasing use of deepfake technology to scam companies. At the moment, their less sophisticated methods of impersonation are working well enough for them. But, as our awareness and defences evolve, so will their methods and the return on investment will become worthwhile for them to start leveraging AI more and more.

Implications of AI for individuals

In October 2022, the Manga artist Chikae Ide revealed that her new work 'Poison Love' was based on her own experience of a romance fraud, possibly powered by deepfake technology. In 2018, Ide was contacted via Facebook by someone claiming to be the actor Mark Ruffalo.

Although she was suspicious, the flattering message caught her attention and she agreed to a video call which reassured her. It has been suggested that deepfake technology was used to impersonate Ruffalo on the video call, convincing Ide so fully that the two got unofficially married online before she ended up wiring him a total of 75 million yen, equivalent to $523,200 over three-and-a-half years. She used her savings, auctioned her artwork, delayed paying bills, borrowed money from friends and spent most of the money she earned from a contract with Gucci.[20] When I spoke with Ruth Grover about romance scams, we addressed the ways criminals will leverage AI to make their scams more convincing – and how some are already doing so:

> 'We always say to people "have a proper video chat, where you can both see each other, you can say something, they answer and you can know they're real" but with AI they are going to be able to do that. But they'll still use formats and scripts, they might be able to manipulate technology and make a really good video call but they will still use the same stories, they will still ask for Bitcoin. We can't depend on the picture or the video to know they're real, we've got to focus on the stories that they tell.'

The methods of scammers often remain the same, even if the medium they use evolves and becomes more sophisticated. Impersonation, social engineering and fraud – whether it is a snake oil sales person travelling from town to town, a phishing email apparently from the boss needing an urgent payment to a new supplier or a deepfake call from an investor to their bank – the

mechanisms scammers use may make their scams harder to see as time moves on, but their strategies and motivations often remain constant, with patterns we can become attuned to.

This chapter began with DeStefano's chilling experience of a deepfake scam that targeted her family. In her testimony she told of how deepfake technology had been used to catapult her into a parent's worst nightmare, until she discovered it was a cruel deception using AI to attempt to defraud her. She commented on how many other individuals she had heard from, who had experienced a similar scam. But the numbers are impossible to know. What we can be sure of is that what is true at the national and organizational level is true for us as individuals, too. Deepfakes may only currently be appearing in edge cases, but we can expect an increase in deepfake social engineering in coming years.

DeStefano is not the only mother who has hit the headlines with a deepfake experience in recent years. In March 2021, Raffaela Spone from Pennsylvania, US, was accused of sending deepfake videos of her teenage daughter's cheerleading rivals to the team coach, seemingly in a bid to use videos of the girls naked, drinking and smoking to ruin their reputations.[21]

However, in this case, it was the deepfake claim – rather than the video itself – which wasn't as it first appeared.

Plausible deniability

The local district attorney and police repeated claims that Spone had created deepfake videos in multiple press

conferences, with one of the girls also making the claim to national press and TV media. However, multiple deepfake creators shared their reasons for believing it was highly unlikely that the videos were deepfakes, with a level of intricacy and nuance that would require a great deal of technical skill to produce.[22] During Spone's trial, evidence emerged that the images were in fact authentic, with confirmation from witness testimonies. In the trial, after the DA and his team admitted they were 'unable to confirm the video was falsified', the cyberbullying claims which related to the alleged doctored photos and videos were dropped. Spone was found guilty of misdemeanour harassment – while she was found guilty of sending harassing messages, it was deemed that the associated video and images were real and not deepfakes.[23]

Welcome to plausible deniability, the deepfake era. With AI facilitating the production of ever-convincing fake images, audio and video, is this the most dangerous element of the advancing technology? The technical seeds of deniability and doubt have already been planted.

With deep implications for bias, discrimination, trust, and the way we perceive reality, along with the force multiplier effect on social engineering, AI poses very real challenges to cyber security not just in the future, but now.

Staying cyber safe in an AI age

When it comes to defence, we are at a challenging time in the AI era, partly because of the exponential growth of the abuse of AI. We have invented skydiving and now we're

rushing to invent the parachute on our way through the skies. However, as much as cyber criminals are exploring how they can use AI, defenders, academics and governments around the world are researching how to defend against such attacks – including using AI as part of the solutions.

At the organizational level, it is important that any AI systems are audited for security and privacy issues and that policies and guidance are created and communicated so that people understand the boundaries of safe AI use at work. Whether in our professional or personal lives, it is advised to avoid entering sensitive information into public LLMs, remaining aware that prompt data may be stored by the provider. We also need to be cognizant that LLMs can make it easier for cyber criminals to gather information on us and to craft more convincing, persuasive, grammatically correct and well-written phishing emails, and messages.

With deepfakes, there are currently some common telltale signs of a deepfake video. Physiological factors can be a giveaway, including if the subject is not blinking, not turning their head or if there are distortions around the face, especially if something (such as their hand) goes in front of their face.

Ultimately, verifying the identity of those we are communicating with is our best line of defence. We cannot trust based on sight and sound alone. The same advice that I have shared for social engineering applies here – be tuned into whether a communication is unexpected or unusual, be aware when your emotional buttons are being pressed

and take a pause to verify identities and information before trusting what you are seeing or hearing.

AI shows how cyber criminals can use technology to evolve their tactics, and we must do the same to advance our defences. The standard advice to check spelling and grammar as a way of spotting social engineering is increasingly unreliable and, even worse, it can give a false sense of security. Likewise, using tools such as reverse image search to screen out romance scammers, or having a video call with new online connections, cannot be relied upon to weed out the fraudsters. When we can't believe our eyes and ears, an anti-scam mindset becomes even more critical.

Notes

1 DeStefano, J (2023) Artificial intelligence and human rights witness testimony, US Senate Committee on the Judiciary Subcommittee Hearing, 13 June. www.judiciary.senate.gov/committee-activity/hearings/artificial-intelligence-and-human-rights (archived at https://perma.cc/PUR6-7E6D)

2 Cooke, R (2023) How scammers likely used artificial intelligence to con Newfoundland seniors out of $200K, CBC News, 22 March. www.cbc.ca/news/canada/newfoundland-labrador/ai-vocal-cloning-grandparent-scam-1.6777106 (archived at https://perma.cc/QP4S-XZ8H)

3 Turing, A M (1950) Computing machinery and intelligence, Mind, 49, 433–60. redirect.cs.umbc.edu/courses/471/papers/turing.pdf (archived at https://perma.cc/89D6-EPUT)

4 BBC News (2014) Computer AI passes Turing test in 'world first', BBC News, 9 June. www.bbc.com/news/technology-27762088 (archived at https://perma.cc/Y4EF-G3NZ)

5 The Glasgow Herald (1940) Senator Marconi's doubts on wireless: good thing for the world or a menace. The Glasgow Herald, 13 May. news.google.com/newspapers?nid=2507&dat=19400513&id=pXFAAAAAIBAJ&sjid=M5IMAAAAIBAJ&pg=3634,4029838&hl=en (archived at https://perma.cc/L9W8-3V28)

6 Bridgewater, S and Robinson, T (2023) Highlights from the RAeS Future Combat Air & Space Capabilities Summit, Royal Aeronautical Society, 26 May. www.aerosociety.com/news/highlights-from-the-raes-future-combat-air-space-capabilities-summit/ (archived at https://perma.cc/QW73-DU6E)
7 Ibid
8 TED Radio hour (2020) Joy Buolamwini: How do biased algorithms damage marginalized communities?, NPR, 30 October. www.npr.org/transcripts/929204946 (archived at https://perma.cc/YP3S-GJM4)
9 BBC News (2018) Amazon scrapped 'sexist AI' tool, BBC News, 10 October. www.bbc.com/news/technology-45809919 (archived at https://perma.cc/E4G3-MGMV)
10 Obermeyer, Z et al (2019) Dissecting racial bias in an algorithm used to manage the health of populations, Science, 366(6464), 447–53 (October). www.science.org/doi/10.1126/science.aax2342 (archived at https://perma.cc/ZK5Y-RW8U)
11 Shead, S (2020) How a computer algorithm caused a grading crisis in British schools, CNBC, 21 August. www.cnbc.com/2020/08/21/computer-algorithm-caused-a-grading-crisis-in-british-schools.html (archived at https://perma.cc/9Y34-WNE4)
12 Hu, K (2023) ChatGPT sets record for fastest-growing user base – analyst note, Reuters, 2 February. www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/ (archived at https://perma.cc/3FQ5-TVBF)
13 Sharma, J and Sharma, R (2017) Analysis of key photo manipulation cases and their impact on photography, IIS University, 6(1), 88–99. iisjoa.org/sites/default/files/iisjoa/2017/PDF/11.%20Jitendra%20Sharma%20&%20Rohita%20Sharma.pdf (archived at https://perma.cc/S8G5-PF63)
14 Farid, H. Photo tampering throughout history. faculty.cc.gatech.edu/~beki/cs4001/history.pdf (archived at https://perma.cc/8ETA-GQR5)
15 Bregler, C et al. Video rewrite: driving visual speech with audio, Chris Bregler. chris.bregler.com/videorewrite/ (archived at https://perma.cc/FY7K-KAYY)

16 Sample, I (2020) What are deepfakes – and how can you spot them? The Guardian, 13 January. www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them (archived at https://perma.cc/N7NE-U3HU)
17 Senatskanzlei Berlin (2022) Die Regierende Bürgermeisterin @FranziskaGiffey: "Es gehört leider zur Realität, dass der Krieg mit allen Mitteln geführt wird – auch im Netz, um mit digitalen Methoden das Vertrauen zu untergraben und Partner und Verbündeten der Ukraine zu diskreditieren", 24 June. x.com/RegBerlin/status/1540375544755355655?s=20 (archived at https://perma.cc/UTM9-325M)
18 Brewster, T (2021) Fraudster clones company director's voice in $35 million heist, police find, Forbes, 14 October. www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=e63f9fa75591 (archived at https://perma.cc/TF5N-2TTD)
19 Stupp, C (2019) Fraudster used AI to mimic CEO's voice in unusual cyber crime case, Wall Street Journal, 30 August. www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 (archived at https://perma.cc/BH8D-KYAW)
20 Takahashi, M (2022) Manga artist falls for Mark Ruffalo, loses $500,000, The Asahi Shimbun, 22 September. www.asahi.com/ajw/articles/14722566 (archived at https://perma.cc/CZZ2-9YQE)
21 BBC News (2021) Mother 'used deepfake to frame cheerleading rivals', BBC News, 15 March. www.bbc.com/news/technology-56404038 (archived at https://perma.cc/P2PE-68CP)
22 De Geurin, M (2023) The completely unbelievable story of the 'deepfake cheer mom', Gizmodo, 3 October. gizmodo.com/deepfake-cheer-mom-sues-for-defamation-1850884295 (archived at https://perma.cc/SG5N-DAKB)
23 Ibid

CHAPTER FOURTEEN

Conclusion: staying safe from cyber attacks

It may seem, after reading some of the incidents, experiences and perspectives in this book, that the balance between cyber security and cyber insecurity always favours the criminals. The challenges we face are complicated and criminals will endlessly aim to evolve and evade detection and controls. However, we must not overlook the progress we have made – and continue to make – in the short history of cyber security. I shared some examples of successful countermeasures, advancements and law enforcement operations throughout this book. When cyber security wins, collaboration is usually at the heart of our resilience.

Digging into the cyber attacks and incidents that hit our headlines could give the impression that there is often a vacuum of consequences for cyber criminals. While we have a long way to go in our fight against cyber crime, that which enables online attackers can also be their downfall, as Benedict Hamilton commented when I interviewed him about his cryptocurrency crime investigations:

> 'They need to have a phone and they need to have a computer. They need to have email addresses. They need to be able to get the value into the digital world and out of the digital world. Their connection to the internet goes through routers that have records and logs. Their use of VPN providers has records and logs. Their security is fundamentally undermined by the digital world because there's just so much record keeping.'

We have a long way to go, and we will require a lot more resources to tip the balance in favour of cyber defence, but the more cyber attacks there are, the more incentive our institutions have to invest in those resources. It will require governments and organizations to invest more deeply. It will also require greater collaboration, ingenuity and big-picture thinking to truly disrupt the mechanisms which power cyber attacks.

If this seems out of the day-to-day control of you or I, then the good news is that we can all take action to make ourselves, our families, our organizations and our communities more secure. Practising foundational security behaviours is key. I have shared lots of advice throughout this book and summarize these foundational security practices as:

1 Protecting devices: physically locking devices with strong passcodes, installing updates as soon as they are

released to fix known vulnerabilities and wiping data from devices before we dispose of them.

2 Protecting online accounts: using long, complicated and unique passwords for all accounts as well as enabling two-factor authentication.

3 Protecting communications: being alert to phishing over all communication channels and being especially attuned to the red flags of communications that are unexpected, make us feel something and ask us to do something.

4 Protecting information: being aware of the information we share and who we share it with, for example on social media, and making sure we back up data as well as disposing of it securely.

5 Protecting our circle: being aware of how cyber criminals abuse technology and practising secure behaviours helps keep our friends, families, neighbours and colleagues stay more secure, too; passing on stories and relevant advice can have a positive ripple effect on those around us.

Spreading the word and helping those around us safely engage with technology helps us all reap the benefits of the internet while minimizing potential harm. As many of the experiences recounted in this book show, the impact of cyber attacks often goes beyond financial losses and can extend to mental and physical harm, too. In some cases, the consequences can be tragic.

Your mindset plays a key role. A common theme of advice from those I interviewed for this book has been 'if it seems too good to be true, it probably is'. While this may seem a little sad, a healthy dose of scepticism goes a long way in cyber security. Taking time to verify someone's identity is unlikely to do any harm, someone trustworthy

and with your best interests at heart won't mind you taking steps to keep yourself safe.

I haven't shared the stories and perspectives in this book to make you paranoid, but rather to help you be aware. Our lives can be enriched by the internet and connected technology, especially when we know the secrets behind cyber attacks and the strategies that help us stay safe.

Index

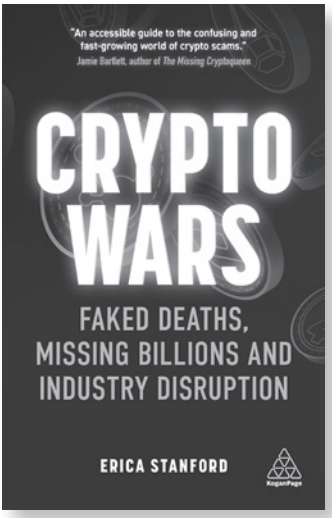
Looking for another book?

Explore our award-winning books from global business experts in Digital and Technology

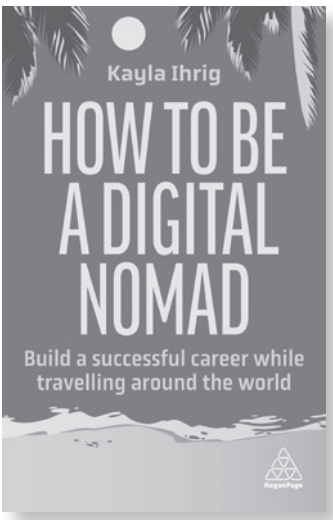
Scan the code to browse

www.koganpage.com/digital-technology

Also from Kogan Page

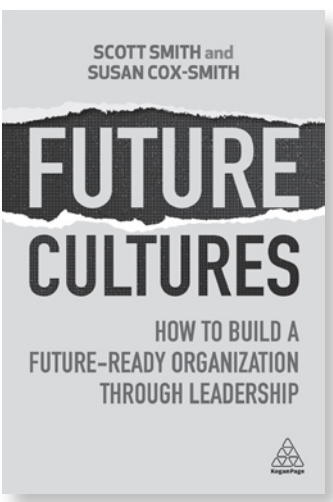


ISBN: 9781398600683



ISBN: 9781398613058

ISBN: 9781398611320



ISBN: 9781398612389

KoganPage

THIS PAGE IS INTENTIONALLY LEFT BLANK

THIS PAGE IS INTENTIONALLY LEFT BLANK