Cybersecurity for Humans

Dr Victoria Baines

9th May 2023

Cybersecurity is nothing more than protecting networks and information. Network and Information Security is precisely what it was called before we got caught up in science fiction hype. In order to protect networks and information effectively, it helps to know what we're defending against. The trouble is that in order to understand cybercrime, we have to learn a new language. Below is a synthesis of terms from three cybersecurity glossaries compiled by the US National Institute of Standards and Technology, the UK National Cyber Security Centre, and cybersecurity vendor Crowdstrike.[1]

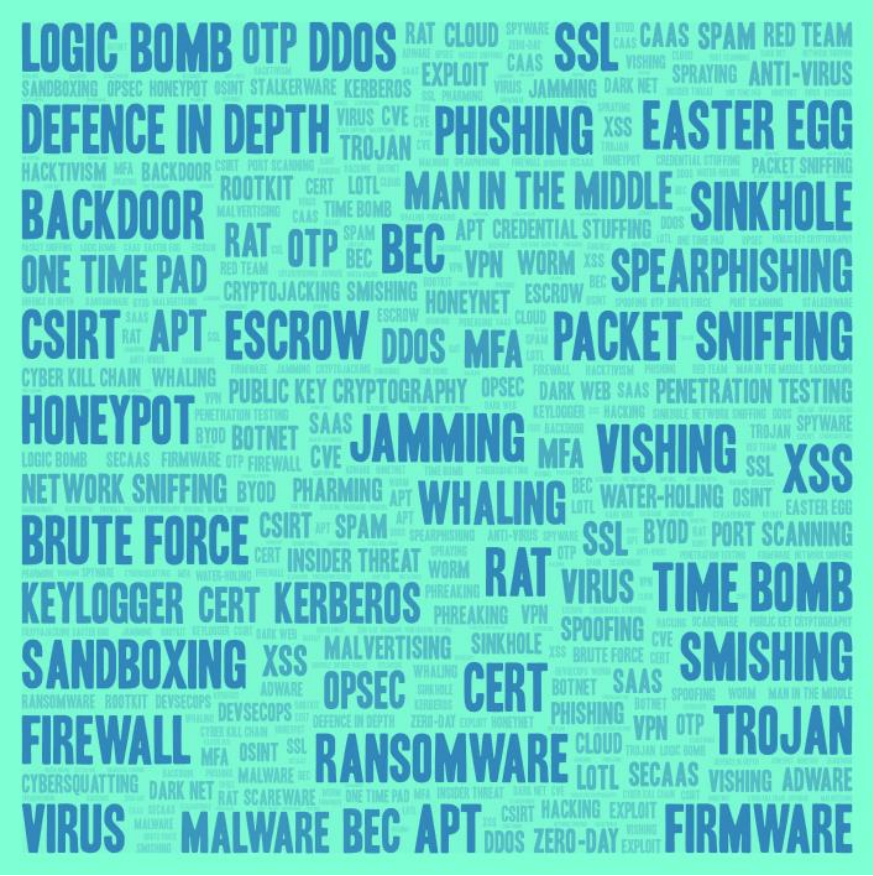

Figure 1 Word cloud of cybersecurity terms, based on three online glossaries

There are discernible patterns, among them a fondness for acronyms. BEC is Business Email Compromise, when someone is tricked into transferring funds or sharing valuable information in response to what looks like an official email from a colleague or business partner. APT is Advanced Persistent Threat, which is a catch-all term for criminal groups who do in-depth research on high-value targets and are able to conduct sophisticated attacks. They are quite often – but not always - funded by or affiliated to national governments.

---

[1] https://csrc.nist.gov/glossary; https://www.ncsc.gov.uk/information/ncsc-glossary; https://www.crowdstrike.com/cybersecurity-101/

DDoS is Distributed Denial of Service. As the name suggests, that's when an online resource like a website stops working because it's flooded with traffic.

Wares, Whales, and Warriors

RAT stands for 'Remote Access Trojan', highlighting another trend of 'Cyberese', which is a penchant for fantasy, myth, and macho military imagery. The 'remote access' part is straightforward. That's when someone gains access to your device remotely. If you work in an organisation with IT support, you'll be aware that your colleagues can do this legitimately when you have a problem – they can take over your desktop and go into your apps and files. But clearly we don't want criminals to do that without our knowledge. That epic word 'trojan' suggests something rather underhand and unseen, Odysseus and the other Greek warriors sneaking into Troy in the belly of the wooden horse. Beware of Greeks bearing gifts, and so on. And that's precisely what a trojan is in cybersecurity. It's a program that seems legitimate but actually contains malicious code, and that hides in plain sight until it is activated.

There are also words here that end in '-ware'. Computing relies on hardware – equipment – and software – programs and applications that run on the equipment. By extension, firmware is software that makes hardware work properly. All of the '-wares' we might encounter in cybersecurity are just portmanteau words, blending software with other characteristics. So malware is an umbrella term for malicious software, ransomware attempts to blackmail the user, and adware describes those nasty pop up advertisements. Using similar logic to different effect, some people prefer to call that malvertising. There's also spyware, which gathers sensitive information without your knowledge; stalkerware, which can track someone's online and offline activity; and scareware, which is malicious software that pretends to be legitimate antivirus software.

We can also see several fish-based terms. In the 1960s and 1970s, early hackers who tinkered with public telephone networks – including Apple founders Steve Jobs and Steve Wozniak - were known as phreaks or phreakers.[2] Over time, this ph- spelling was transferred to other words beginning with f-, including pharming, which is when internet users trying to reach a legitimate website are redirected to a criminal one; and, of course, phishing, which describes a number of different ways of luring us into sharing sensitive information or taking a particular action.

Phishing is perhaps the best known manifestation of social engineering, manipulating people into unwittingly facilitating a cyber-attack against them or another target. Because the tactic is one of catching people on a hook, and of victims taking the bait, the vocabulary plays on the association with angling. So we have SMiShing, when phishing communication is sent by SMS/text message, and Vishing, by voice message. There is also spear-phishing, which is targeted at a particular individual, and designed to look like it's from a person they already know or trust, and whaling, aimed at 'big fish' senior executives.

How Cybercrime Works

In the previous lecture, *Defeating Digital Viruses*, we considered botnets (another portmanteau word!), networks of infected devices that are then used to conduct attacks on other devices, systems or networks. We discovered how our devices can become part of a botnet when we click on malicious software, which often arrives in an attachment in a message, or a web link of some description. That malware then infects our device, hijacking the processing power to disable websites by flooding them with traffic (Distributed Denial of Service). Not downloading the malware in the first place is the surest way to prevent the device being infected and used in attacks. For all that cybercrime relies on being able to exploit technology, most of the time it doesn't succeed – and importantly doesn't pay – if we don't play along.

Social engineering is crucial to the success of most of the cybercrime we encounter in our daily lives, unless we're responsible for managing large IT networks. When criminals send a phishing email offering us money or a prize, they use the same tactics as legitimate advertisers. They play on our desire to acquire and to be that little bit better off. Their offers are very often urgent and time-bound, just like the proverbial furniture discount sale that must end Sunday but never seems to. Just as we have become wise to the 'hard sell' tactics of the vacuum cleaner salesperson dumping a pile of dirt on the carpet, creating a problem so that we are reliant on them to fix it, or the door-steppers who keep talking until we comply with their wishes, we can apply similar defensive measures against anyone who wants us to click on a web link, open an attachment, transfer money, or disclose our personal data.

---

[2] https://www.theatlantic.com/technology/archive/2013/02/the-definitive-story-of-steve-wozniak-steve-jobs-and-phone-phreaking/273331/

If someone you didn't know rang your doorbell and asked if you would like a free iPad, a million pounds or to have sex with them, you would have your suspicions about their motives and the legitimacy of their request. But for some reason we find it harder to do that when we receive an email or chat message, or see a flashing advert, or hear a voicemail message. Why is that? We have had thousands of years of practice defending our homes. But technology is inside our homes, which many of us perceive to be a safe space where we can let our guards down. They are our fortresses, protecting us from the dangers of the outside world. Earlier in my career when I investigated online offences against children I was struck by the number of parents who told police and the media that they had thought their child was safe because they were in their bedroom. That is not to say that children are always 'unsafe' when they use IT – far from it. But it is, I think, an illustration of our association of home with safety.

Even when we are distant from that safety, technology is often our assistant, helping us navigate, keeping us informed and entertained, connected and enabled. It's an essential service. It's in our trust bubble. It's why people follow sat navs to the edge of a cliff and why people in some countries call the emergency services when Facebook goes down. IT has already become an extension of us – our capability, our intellectual capacity, our bodies. Along with our five senses, it is now part of each of our toolkits for navigating daily life and the world around us. It amplifies, enhances, even compensates for those senses and faculties. I used to remember phone numbers, but now my phone does that for me. Computer vision allows people with impaired eyesight to appreciate images on social media through automated audio description. Automated closed captioning of TV shows and meeting transcription supports those who are hearing impaired. Many of us no longer consider technology to be something that is apart from us. It is already in our personal space, which can make it harder to question.

For others, conversely it may be the *unfamiliarity* of technology that makes them less confident in acting on their suspicions. Novelty can be as frightening as it is exciting. That's particularly important for us to recognise in light of the fact that scaring us is a key tactic of cybercriminals and a common feature of their business model. They play on our fears for our safety and of loss, but also of being found in the wrong. Ransomware is profitable because it threatens people with the loss of all their data. Businesses understandably perceive this as catastrophic if they don't have a backup system. The threat of that loss may be sufficient for them to pay the ransom, which doesn't guarantee that access to the data will be returned.

In 2010, when I was working for the European police agency EUROPOL, we started to see reports of police-themed ransomware. This locked computers and demanded a fine as penalty for illegal activity, typically related to serious crimes such as child abuse and terrorism. The pop-up lock screen always included a deadline for payment, use of legitimate logos and branding to lend an air of authenticity, and quoted (often incorrect) legal statutes. The IP address and location of the victim's device was often displayed, adding to the impression that they were under official surveillance. It didn't have to be accurate to be persuasive, and it didn't matter that this information was easy for anyone to capture. The threat to victims was not just that they would lose their data but that they would be arrested if they didn't comply. This approach relies on the threat and the sense of urgency outweighing our suspicions. It makes us suspend our disbelief. It makes us forget to question what we normally would, such as why the police is asking us to pay a relatively small fine (£200) for serious crimes. But once we know how the scam works, it immediately becomes easier to spot.

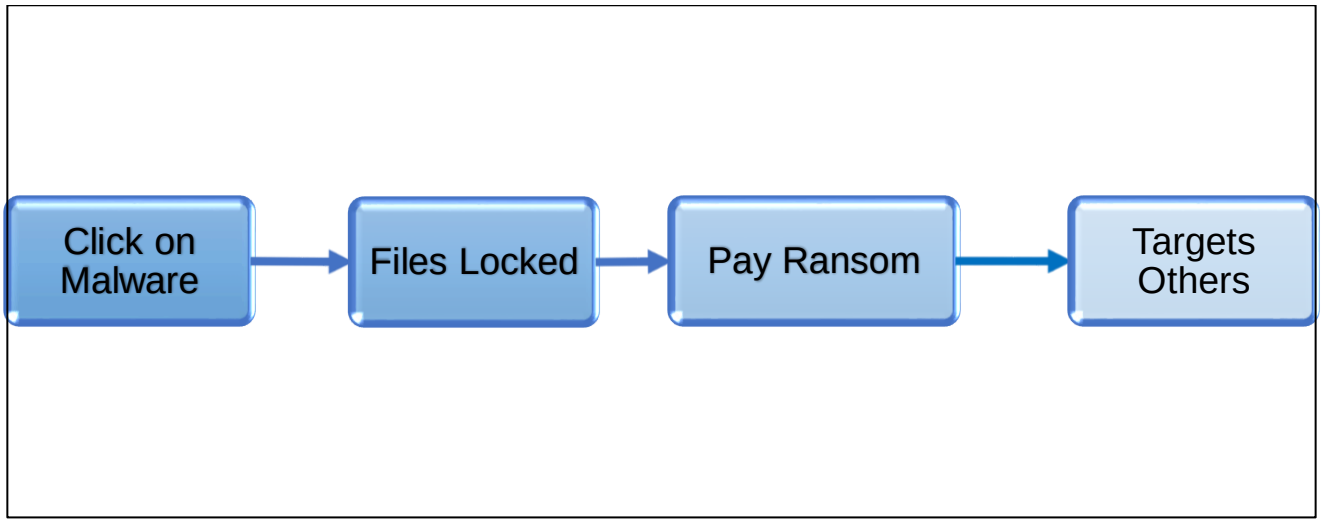

Figure 2 The Ransomware Business Model

Even if only a few of us pay the ransom, the criminal makes a profit. Over the years the tactic has evolved, so that small and medium sized businesses are issued ransom demands of thousands of US Dollars, while large corporations may be targeted for millions. Insurance companies now include payment of ransoms in their cyber risk policies for businesses. This is highly controversial, because paying the ransom directly funds organised crime and rogue states with oppressive regimes. Law enforcement agencies naturally do not want criminal groups to make any more money, and the US government has even suggested that victims who pay the ransom may be liable to prosecution.[3] It's my opinion that it's part of our civic duty not to pay the ransom. But I do understand why people and organisations of all sizes ultimately choose to pay. What are the alternatives?

Checking Senders and Links

Prevention is naturally better than cure, and the ideal state is that we use our critical thinking to not click on links or attachments that download malicious software. If someone came to your door claiming to be a police officer or another official, you would ask to see their ID. If someone sends you an unsolicited email or asks you to click on a link, you can follow exactly the same procedure. Checking just two things in any email can prevent you falling victim to a number of cybercrimes. It's simply a question of developing the habit of i) looking at who the message is really from and ii) checking where they really want to send you.

The email account sending the message may be different from the display name you see. Depending on the device, app and email service you use, you can reveal the real address by hovering over the display name, right clicking on it, or pressing and holding on it. If a message directs us to click on a link, we can check the real link behind the display text using similar methods, which vary based on the device and apps you use. If *either* the email address or the links in the message don't look right, don't click! Take a minute to do some more research. For example, I often Google the body text and links from messages that I suspect, to see whether other people have reported them as scams.

Technology helps us with this. Large email providers such as Microsoft and Google use a combination of filters to identify a message as 'junk', including content filters that flag some of those formulaic features of scams such as urgency and unsolicited sexual content; blacklists of senders and known 'bad' IP addresses; and Bayesian filters, that learn for instance when you consistently mark email from a particular sender as spam. Routing a message to the Junk folder is Outlook's or Gmail's way of telling you there's something about it that may not be entirely legitimate. Your provider may also prevent certain content from loading in messages marked as Junk, so that you don't inadvertently click on it. This creates a critical distance between you and the criminal.

Government services, banks, and delivery companies often use SMS text messaging to send us short updates, and we've naturally seen an increase in criminals posing as those services to scam people. Cybercriminals also exploit whatever is topical, so inevitably there has been an increase in Covid-related scams in the last few years. A popular one at the moment purports to be from the child of the recipient, sometimes in distress and sometimes asking for money. For all three of these message types there is an obvious way to verify who they have really come from, and that is contacting the official source. There is always something we can do to double check. We just need to resist the temptation to be convinced in the moment that we need to comply immediately.

Keeping Software Up to Date

But what if a message has made it through the filters and you have already downloaded malware? That's where antivirus software comes in. Even if you click on a suspicious link or attachment, the malicious program can be detected and removed before it can do any damage. A good antivirus tool will scan files as they enter your device and scan programs already on your device. It then compares both to data and signatures for known malware, and removes or quarantines any for which it gets a hit. There are some good free options available, but also increasingly this kind of protection is incorporated into operating systems for devices. New malware variants are constantly appearing, which means antivirus libraries are constantly being updated, and new security vulnerabilities are continuously discovered. This means that it's very important to keep the operating systems on our devices up to date, as well as having antivirus software.

A striking illustration of what can happen when software isn't kept up to date is the WannaCry ransomware attack of 2017. It has since been attributed to 'affiliates of the North Korean government', and it infected

[3] https://ofac.treasury.gov/recent-actions/20201001

computers in more than 150 countries.[4] It led to the declaration of a major incident in the UK's National Health Service.[5] But the NHS wasn't the target. It was impacted purely because some NHS trusts had not kept the operating software on their computers up to date.

Already there are millions of us who have pacemakers, continuous glucose monitors, and insulin pumps that are connected to the Internet, and which use our home and mobile connections to report to our medical providers. Even more of us use mobile apps to improve our mental health and well-being. The potential impact of that service being interrupted, or a criminal getting hold of and exploiting that very sensitive data, extends beyond financial loss and mere inconvenience. If our healthcare relies on our connection to the Internet, we should all be stepping up to do whatever is necessary to secure that by making sure that the software on our devices is up to date.

Different, Strong Passwords

Some phishing messages are designed to trick you into sharing your login credentials with criminals. Any cybercriminals worth their salt will try to access multiple services with one set of credentials. If you have the same password for all your accounts, one leaked password could give a criminal access to everything else.

If you think criminals may have gained access to your financial data – for example bank account or credit card details – you should always contact those providers so that they can be aware of any suspicious transactions, even if you haven't seen any money leave your accounts. And any time that you know that have been the victim of cybercrime, you should change the passwords for the accounts that you think might be affected.

There is ongoing debate about the rules we should be using for choosing our passwords. Many websites and apps force you to use a combination of letters, numbers and symbols, while government agencies and cybersecurity specialists recommend three random words. Regardless of the format, make sure it's not something a criminal can guess, such as the name of your pet and the year of your birth. Criminals trawl social media for that kind of information. You should also think twice before taking part in quizzes on social media for that very reason.

haveibeenpwned.com is a legitimate website where you can find out whether any of your login credentials have been involved in a data breach. It's sometimes a sobering experience to input one's email addresses and phone numbers and see the results. While you should always change your passwords regularly in any case, knowing exactly which accounts require an urgent change can be very helpful.

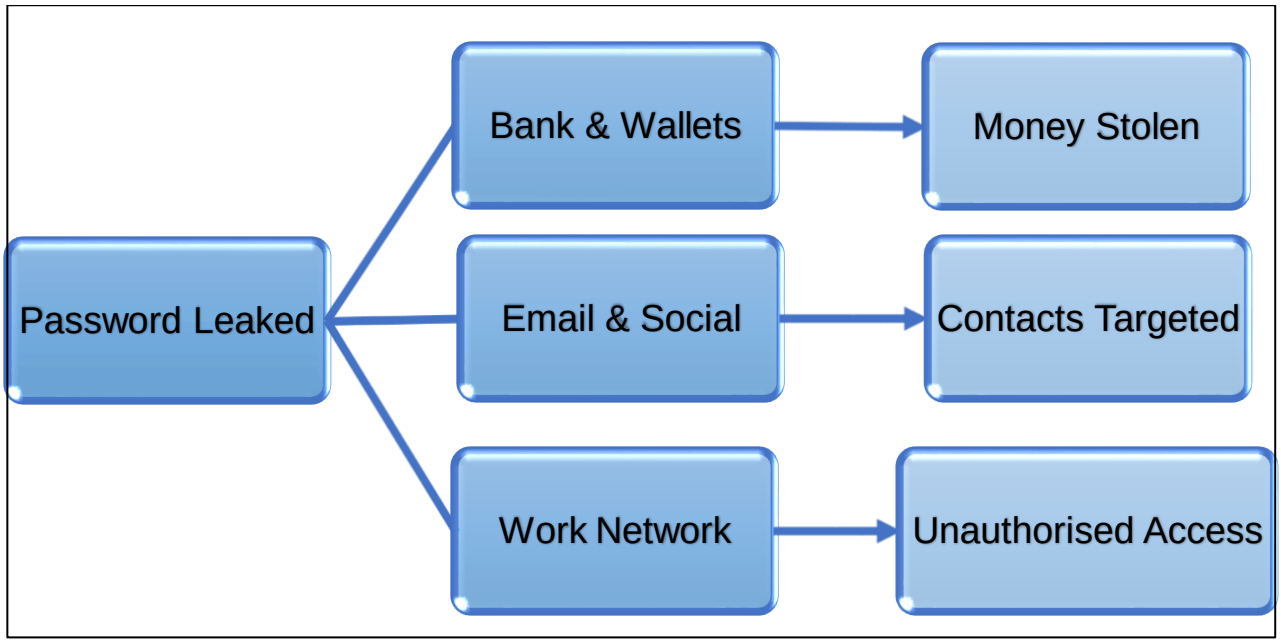

Figure 3 The unfortunate consequences of having the same password for different services

[4] https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
[5] https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

Passwords should be something that only you know. But we can also make use of things we have, such as our phones, a smart card or a card reader, and things we are, such as fingerprints, facial recognition, and other biometrics. This is known as Multi Factor Authentication (MFA), and it reduces the risk of criminals getting into an account because it requires more than one type of authentication. So, the facial and fingerprint recognition features on mobile devices use something the owner is biometrically to unlock a store of passwords for online services. Equally, it has become routine for banks and other services to send a verification text whenever a customer tries to log in with a password. The minor inconvenience of inputting an extra security code makes it much harder for a criminal to hack into an account.

There's no denying that regularly changing different passwords presents something of a practical challenge given the number of social, financial, medical, government, retail and other accounts most of us have. Here, too, there are technical solutions. Dedicated password manager apps are widely available, and increasingly web browsers and device operating systems offer to store passwords for you so that you don't have to remember them all.

Just Three Things?

Throughout this lecture series on *Humanising Cyberspace* we have seen how the benefits of Information Technology, along with its problems and their solutions, all entail a dynamic relationship between people, process, and technology. This applies as much to cybercrime as it does to how we govern the Internet, how we tackle fake news, and how we behave towards each other in connected spaces.

Because so much of the cybercrime to which most of us are exposed in our daily lives relies on our being manipulated - on social engineering – there are concrete steps that we can all take to significantly reduce the risk of falling victim. We can get into the habit of checking just two things: where a message really comes from, and where web links really go to. In doing so we address the human vulnerabilities, the people part, and we put to good use that healthy suspicion that has served us well for millennia. We can ensure that when it comes to passwords, we have a digital housekeeping process that prevents criminals guessing our credentials and re-using them to cause us further damage. Finally, by installing antivirus and keeping other software updated, we can make use of technology that is designed to defend us against attack.

There is no such thing as absolute cybersecurity. But with these three things, we really can arm ourselves against the vast majority of cybercrimes we currently encounter as citizens. With these three things, we really can stop criminals hijacking our devices, stealing from us, and holding us to ransom. Just as importantly, we can protect our family and our friends. So, this is a call to action: once we've done these three things for ourselves, let's go out there and show everyone else how to do it, too.

Resources

The UK National Cyber Security Centre's "Top tips for staying secure online" runs through all the basics covered in this lecture, such as passwords, software updates, and multi-factor authentication - https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

There's a lovely clear infographic on how to do deal with phishing emails here - https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf

The NCSC also provides a glossary of cyber security terms - https://www.ncsc.gov.uk/information/ncsc-glossary

A similar glossary can be found on the website of the US National Institute of Standards and Technology (NIST) - https://csrc.nist.gov/glossary

The websites of some major banks provide helpful safety and security tips, among them:

- HSBC: https://www.business.hsbc.uk/en-gb/campaigns/bib-help-centre/staying-safe-online . HSBC also has a free Fraud and Cyber Awareness app on the iOS and Android app stores.
- Barclays: https://www.barclays.co.uk/fraud-and-scams/Cyber/stay-safe-online/

A number of the biggest social media platforms have help centres that show you how to change you privacy

and security settings, including activating multi-factor authentication:

- Facebook: https://www.facebook.com/help/235353253505947/?helpref=uf_share
- Instagram: https://help.instagram.com/369001149843369/?helpref=hc_fnav
- TikTok: https://www.tiktok.com/safety/en/privacy-and-security-on-tiktok/
- Snapchat: https://help.snapchat.com/hc/en-gb/articles/7012304746644-How-to-Stay-Safe-on-Snapchat

The No More Ransom project provides information on ransomware, and tools to unlock your devices if you're unlucky enough to be a victim - https://www.nomoreransom.org

haveibeenpwned.com is a legitimate website where you check whether your email addresses and phone numbers have been leaked in a data breach.

Legitimate organisations often share updates on known scams impersonating them. A quick Google is often all it takes to confirm whether something you have received is a scam or not. For instance, in the UK HMRC has a list of text messages that it regularly sends to taxpayers - https://www.gov.uk/guidance/check-if-a-text-message-youve-received-from-hmrc-is-genuine

Further Reading

Jessica Barker (2020) *Confident Cyber Security: How to Get Started in Cyber Security and Futureproof Your Career*. Kogan Page: London. Script

Misha Glenny (2011) *DarkMarket: CyberThieves, CyberCops and You*. Vintage: London.

Edward Lucas (2015) *Cyberphobia: Identity, Trust, Security and the Internet*. Bloomsbury: London.

Geoff White (2022) *The Lazarus Heist - From Hollywood to High Finance: Inside North Korea's Global Cyber war*. Penguin: London.

The Lazarus Heist podcast is also available on BBC Sounds - https://www.bbc.co.uk/programmes/w13xtvg9