Cybercrime Warfare Against People: Pessimistic Side of Online

João Conceição

[1]Universidade Lusófona do Porto, 4000-098 Porto, Portugal
joaodiogocosta@hotmail.com

Abstract. The Internet and its inherent liberating properties, allow people to indulge in their imagination and do things that otherwise would not be possible, including deviating, perverse and dangerous activities.
Cybercrime is a term used to describe criminal activities involving a computer, networked device, or a network, and it can be done not only to companies and institutions but also to individuals.
Even though cybercrime constitutes nowadays one of the biggest threats for financial markets, it's undervalued by a numerous amount of the institutions, with studies showing that the efficacy and recurrence of these attacks do not seem to be decreasing, even with all the awareness being done by cybersecurity institutions.
There are various types of cybercrime, and an abundant share of them include social engineering, which is the art of manipulating and persuading an individual to reveal confidential information, so, by understanding not only the mechanisms behind these attacks, but equally important, the psychological factors as to why people still fall for these attacks, a list of preventive measures can be developed to hopefully guide people in this cybercrime warfare.

Keywords: Internet, Cybercrime, Psychological, Social Engineering, Confidential, Preventive Measures, Awareness, Crimes

1 Introduction

The usage of the Internet became in the last couple of years so ingrained in society, that almost every industry and field of work adapted their way of conducting and superintending businesses to accommodate and take advantage of the potential a vast network that connects people all over the world can offer [1].

Although the Internet is nowadays used by everyone, its concept is still vague for the vast majority of people. For some individuals the Internet is used for entertainment purposes, for others constitutes a source of information and learning, but for almost everyone, remains something mysterious, incomprehensible and for those who know what truly can be accomplished with a networked system like this, frightening. With the growth of the Internet, emerged the possibility of committing crimes digitally. Crime and those who practice it, evolved in order to obtain the most out of their surroundings. Before the post-modern age, all the material assets were possessed in physical form and therefore the crimes committed, involved most of the time the threat of violence and physical force. These methods carried greater risks to those who committed them, as the perpetrators were frequently caught in the act and therefore arrested.

With the digitization of people's owned assets and information, criminals no longer need to reveal their identity as everything can be made anonymously [2], also the act of Social Engineering became much more accessible as a consequence of the multitude of methods there is to persuade and to reach people, such as emails, links, advertisements and blackmail threat [3].

2 Cyberattack Methods and Motivations

Prior to examining and understanding the different types of cyberattacks and possible mitigation/awareness techniques, we need to understand how these attacks are being done, why are they being done and lastly why are people falling for them, as people represent the not only the biggest direct threat to computing infrastructures since the attacks are being committed by people themselves, but also the biggest flaw when it comes to protecting these systems due to their vulnerability to psychological manipulation.

2.1 Social Engineering

Social Engineering is without a doubt the one of the main culprits behind this warfare as 99% of all cyberattacks use social engineering techniques [4]. This simple, yet extremely effective method explores the vulnerabilities of the human mind by strategically persuading one, using most of the times the promise of something as all human activity is prompted by desire [5]. There are various ways of schematizing the process of Social Engineering, but the most common model is Kevin Mitnick's social engineering attack cycle [6].

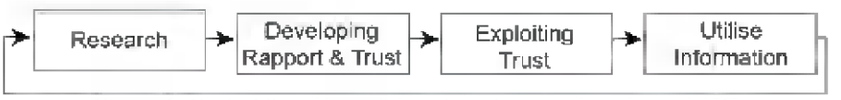

Figure 1. Kevin Mitnick's social engineering attack cycle model[6]

This model divides the process of Social Engineering in 4 parts:

Research. In this phase the attacker will try to gather as much information as he can about his target, this includes the victim's tendencies and vulnerabilities so that he can personalize his attack to his specific victim or victims.

Developing Rapport & Trust. In order to obtain information that in normal circumstances would be unobtainable, the attacker must develop a relationship with the victim, this is usually done with information gathered in the Research phase, for example, if the attacker knows that the victim likes animals and usually donates to animal shelter institutions, then he can impersonate someone from these institutions, giving a false sense of security to the victim.

Exploiting Trust. After developing a 'trustful' relationship with his victim, he can now lure her into giving away personal information or valuable assets.

Utilize information. Finally, with the information gathered, the attacker can now proceed with his attack without needing to interact with its victim any longer, and ultimately reaching his initial goal.

2.2 Types of hackers and their motivation

When we think of a cyberattack, we immediately think of something negative, with the name "cyberattack" in itself having a pejorative connotation, but this is not always the case. Frequently, the means and intentions of an attack are indeed wrong, but in some cases the intentions behind an attack are morally correct. With this being said, we can divide hackers and their ethical reasoning by using the "hat" terminology.

Figure 2. Scheme with the different type of hats[17]

White Hat Hackers. Hackers who "wear" the "white hat" constitute in their current field of activity, the group of hackers that are driven either by positive ethical motivations by their compromise with another company or institution to do the right type of attacks. One particular aspect to note is that, a considerable amount of these

hackers, especially those who work for a company or an institution, were once black hat or grey hat hackers, but were persuaded by these companies to use their expertise in exchange for money or some other type of extrinsic value asset, an example of this is Hector Xavier Monsegur, that worked with the FBI to help prevent and disrupt over 300 hacks in exchange for being released from prison[7].

Grey Hat Hackers. When it comes to Grey Hat Hackers, as with the mixture of both the black and white color, they behave with both white and black hat hacker tendencies, unlike black hat hackers their intentions are usually morally correct, but their means are usually unethical, an example of this, is a hacker who breaches a company network system without their permission, but then reports it to the company in order for them to fix their security flaws.

Black Hat Hackers. Black Hat Hackers are the ones we are going to target our focus to in this paper, they are the polar opposite of White Hat Hackers in the sense that, not only are their means of hacking into a system unethical, but so are their intentions, as they can release malware into a system, steal or hold someone's files and information by ransoming them. An example of a Black Hat Hacker is Kevin Mitnick, who was once the most wanted cybercriminal in the world having stolen millions of dollars from multiple companies. He was later convicted and eventually became a consultant and a writer (White Hat Hacker) [8].

Blue Hat Hackers. Blue Hat Hackers are security professionals whom companies and institutions often invite to check for vulnerabilities in their system.

Green Hat Hackers. Green Hat Hackers are seen as the "newbies" of the hacking community. They're still very much oblivious when it comes to the consequences of their actions, and therefore considered dangerous.

Red Hat Hackers. Just like white hat hackers, red hat hackers also have morally correct intentions in the attacks they commit, but contrary to white hat hackers, the routes they use are usually illegal, that's why they are often referred as the "Robin Hood" of hackers.

3 Cybercrime types, data and preventive measures

According to estimates from Cybersecurity Ventures, it is estimated that attacks like Ransomware happen every 11 seconds, and that across 10 countries, 330 million people have been victims of cybercrime in 2020 [9], with less than 0.05% hackers getting caught and convicted, that results in about 314 million cybercrime attacks made in 2020 in which the attacker was never caught, furthermore, a considerably high amount of cyberattacks aren't reported. It is also important to note that, when it

comes to cybercrime, there are serious jurisdiction issues, as in some cases law enforcement gather sufficient evidence about the perpetrator, but then lack the legal permission to arrest him.

To support the data evaluated in the next topics, a computer questionnaire was conducted by me, João Conceição and João Sebe. The survey was answered by 253 respondents of all ages and genders that use or have used a networked device at some point in their lives. The questionnaire included questions regarding the amount of effort the respondents put on security measures, the types of attacks they suffered and the preventive measures they adopted after such attacks.

3.1 Most common types of attacks

There's a multitude of types of cyberattacks, however some are much more prevalent and/or targeted to a specific demographic. According to the FBI's Internet Complaint Center (IC3) reports, there has been a significant increase in specific types of cyberattacks in the last couple of years [10], this is believed to be caused by the COVID-19 pandemic outbreak, where hackers have personalized their way of committing these crimes in order to obtain the most out of the current situation.

By Victim Count			
Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	241,342	Other	10,372
Non-Payment/Non-Delivery	108,869	Investment	8,788
Extortion	76,741	Lottery/Sweepstakes/Inheritance	8,501
Personal Data Breach	45,330	IPR/Copyright and Counterfeit	4,213
Identity Theft	43,330	Crimes Against Children	3,202
Spoofing	28,218	Corporate Data Breach	2,794
Misrepresentation	24,276	Ransomware	2,474
Confidence Fraud/Romance	23,751	Denial of Service/TDoS	2,018
Harassment/Threats of Violence	20,604	Malware/Scareware/Virus	1,423
BEC/EAC	19,369	Health Care Related	1,383
Credit Card Fraud	17,614	Civil Matter	968
Employment	16,879	Re-shipping	883
Tech Support	15,421	Charity	659
Real Estate/Rental	13,638	Gambling	391
Advanced Fee	13,020	Terrorism	65
Government Impersonation	12,827	Hacktivist	52
Overpayment	10,988		

Figure 3. Most reported cyberattacks to the IC3[10]

As we can verify, Phishing/Vishing/Smishing/Pharming stands out from the ot cyberattacks when it comes to the victim count, with an increase of occurrences over 12 times in the last 5 years [11]. Non-Payment/Non-Delivery and Extortion also experienced significant increases of cases reported in the last 5 years.

Survey Analysis. From the 253 respondents, 52 (20.6%) suffered from a cyberattack at some point of their lives, with the most common one being, Phishing/Vishing/Smishing/Pharming as expected (48.1%) followed by Harassment/Threats of violence (36.5%) and then Non-Payment/Non-Delivery (38.5%).

Note that the respondents could submit multiple answers, therefore the percentages don't add up to 100%

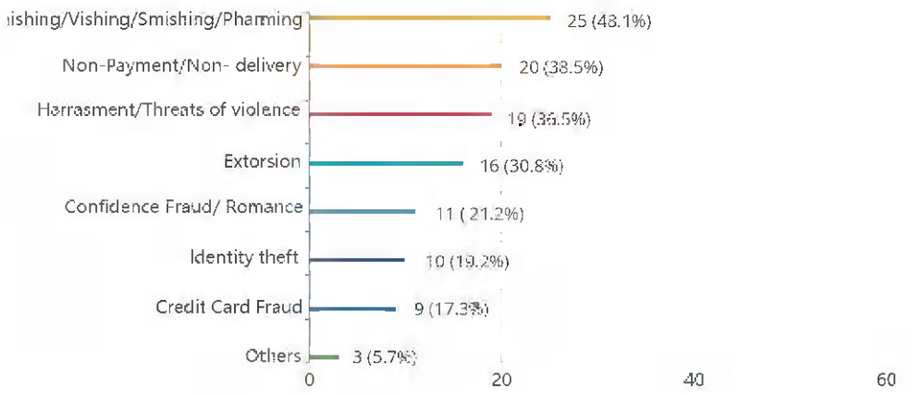

Figure 4. Most common cyberattacks according to the executed survey

As expected, Phishing/Vishing/Smishing/Pharming remained the most common cybercrime in the studied demographic, reinforcing the danger that this specific social-engineering act constitutes not only to individuals but also institutions and companies.

3.2 Cybercrime's financial damage and main targets

Cybercrime's industry seems to be growing each year without signs of stopping, the financial damages caused by cyberattacks are predicted to total $6 trillion USD globally in 2021, to put this in perspective, if cybercrime was a country, it would be the third-largest economy after the U.S. and China [12].

When it comes to attacks on individuals, security firm Norton estimates that in 2017 the total losses added up to $172 billion from 978 million people in 20 countries [13], moreover, last year according to the FBI's 2020 Internet Crime Report, the total losses in the US surpassed $4.2 billion, with approximately 43% of those losses ($1.8 billion) being from victims who were 50 years or more [11]. This statistic becomes even more worrying, when u consider that the percentage of people that are 50 years or older using technological devices is much lower than those who are under 50 years. The reason for this demographic preference is mostly due

to the fact that older people are generally less informed about the danger of using the Internet, and therefore more ingenuous when it comes to these attacks, but also due to the fact that they generally possess more financial resources[14].

The following scheme indicates the total losses in each of the 20 countries, represented in billions (USD).

Figure 5. Estimated losses for each of the 20 countries (Billions)[11]

This following scheme indicates the total victim losses for each type of cyberattack according to the IC3[11].

By Victim Loss			
Crime Type	**Loss**	**Crime Type**	**Loss**
BEC/EAC	$1,[illegible]	Overpayment	$51,[illegible]2
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

Figure 6. Estimated victim losses for each type of cybercrime[11]

Survey Analysis. From the 253 respondents, 52 (20.6%) suffered from a cyberattack, surprisingly enough, from those 52 people only 3(5.8%) were from people aged 50 years or older, therefore, this means that according to the survey, respondents that were under 50 years suffered 16.3 times more cyberattacks then those who are 50 years or older. But if we already established that the older demographic is much more vulnerable to cyberattacks, why does the survey tell us otherwise?

Possible reasons:

- The amount of time spent on networked devices is much lower on the senior demographic.

- Due to their naivety in the field, they might not realize when they suffer from a cyberattack.

It is also important to note that from these 3 people, all of them (100%) reported financial losses when they suffered from a cyberattack.

Note that the respondents could submit multiple answers, therefore the percentages don't add up to 100%

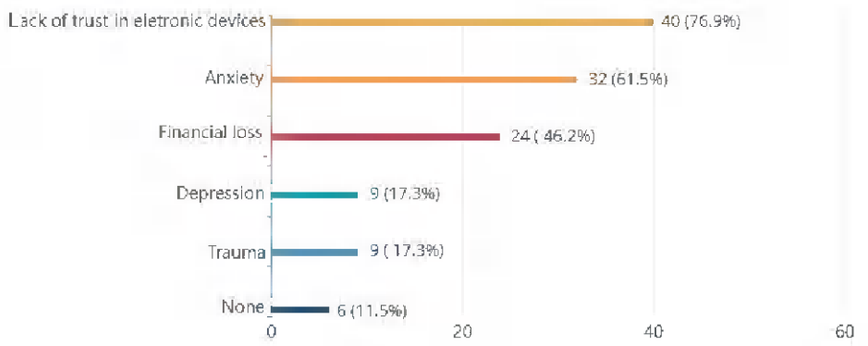

Figure 7. Consequences of the occurred cyberattack in the life of the respondents

3.3 Preventive measures

While it remains almost impossible to stop hacking attempts, we can preemptively adopt ways of conducting our internet usage so that those attempts never become successful, moreover we need to raise awareness to the dangers of conducting improper usage of personal/workstation devices by establishing the biggest telltale signs of a potential cyberattack attempt.

From the infinitude of ways to perform a cyberattack, the following list identifies the more commonly used methods to install malware into your devices and/or obtain access to personal information:

Email Phishing. 96% of all phishing attacks derive from fraudulent emails [15], with 1 in every 4200 emails corresponding to a phishing email [16]. These emails tend to mimic known banking or social media companies, and often claim there is a

problem with your account to incite you to click on a specific link or to share personal information.

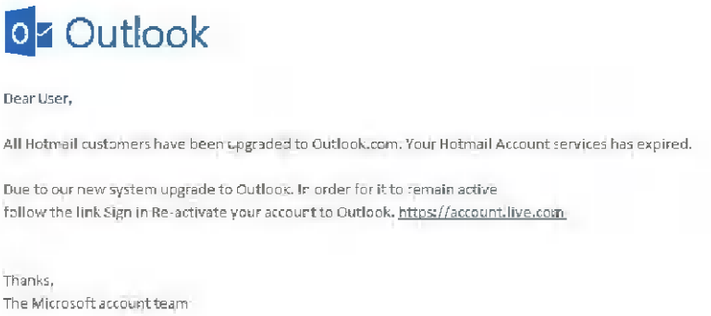

Figure 8. Email Phishing example

Email Phishing preventive measures:

- Never open links from emails you don't know or from companies you don't have an account on.
- If you have an account on the claimed company but you remain unsure whether it's safe or not, contact the company using a phone number or a website you know it's real.
- Check for grammatical errors in the email's content.

Website spoofing. Just like emails, websites can also try to impersonate known companies. This is especially common in online banking services, where the insertion of bank account information is common.

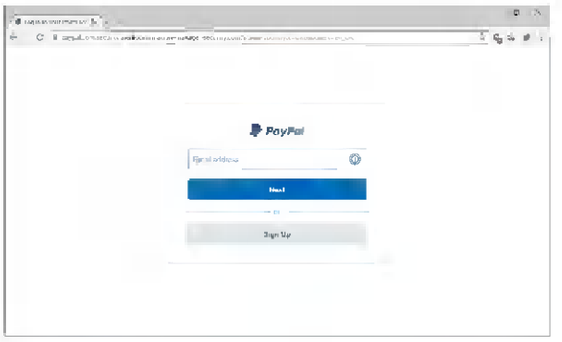

Figure 9. Website spoofing example

10

Website spoofing preventive measures:

- Check for suspicious patterns in the website's address. Usually when a website is trying to impersonate a legitimate company, it will have a very similar address but with slight changes.

- With the introduction of free SSL services, the green lock icon present in the search bar doesn't indicate the website is safe any longer, therefore, you should also check the certificate properties to verify the issuer legitimacy.

- Verify if softwares used to autofill login credentials work on the website you are trying to access, as these usually don't work on spoofed websites.

Malicious ads and pop-ups. Some websites are full of ads and pop-ups with sensationalist messages and images, that are strategically placed so you must press over them to access the website's functionalities. An example of this are invisible ads and pop-ups that are placed over a video player in free movie streaming websites. While most of these ads and pop-ups have the sole purpose of generating revenue, some can install malware into your computer or mobile device.

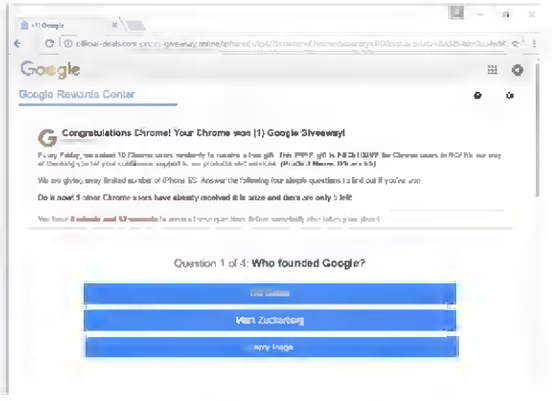

Figure 10. Malicious advertisement example

Malicious ads and pop-ups preventive measures:

- Avoid visiting suspicious websites altogether, as these are the one who usually contain malicious ads and pop-ups.

- On the Internet, general rule of thumb is, if it's too good to be true, then it probably is. Never click on something that claims u have won something.

- Use a trusted ad-blocking extension in your browser, which as the name suggests, blocks ads from showing up on your screen.

Survey Analysis. Having identified the most common ways a cyberattack can be made, and some preventive measures for each one of them, a few questions regarding the security measures people use and the willingness to add new ones were asked in the survey.

According to the retrieved data, from the 253 respondents, 64 (25.3%) believe their personal information is properly secured, 81 (32%) say they don't know and 108 (42.7%) say they don't think their personal information is safe from cyberattacks, conversely, 243 (96%) respondents said they feel like they could improve their security measures, however 169 (66.8%) consider the means to implement more advanced security measures inconvenient.

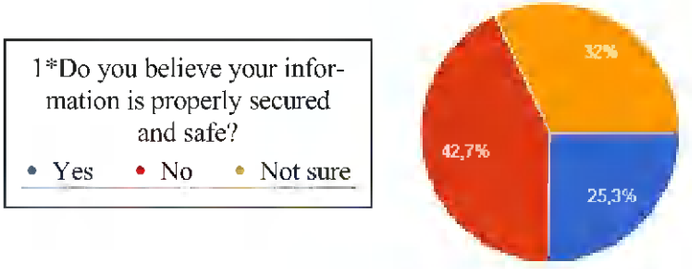

*Figure 11. Pie Chart 1**

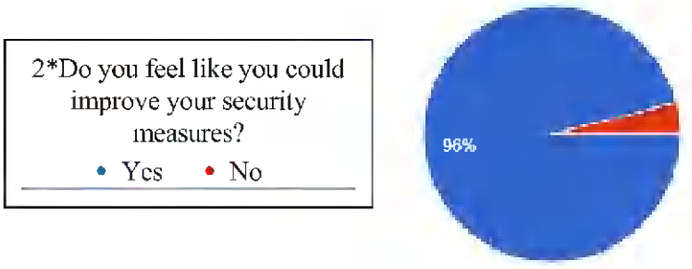

*Figure 12. Pie Chart 2**

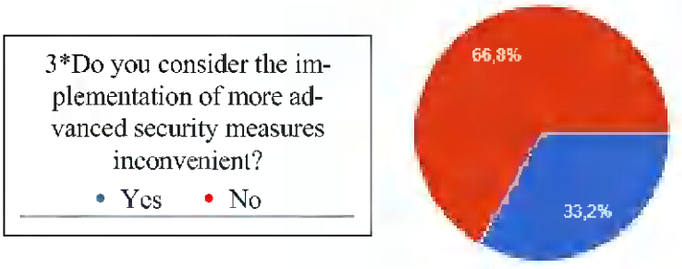

*Figure 13. Pie Chart 3**

4 Conclusion

The catastrophic effects of cybercrime were substantiated in this paper, eventuating not only massive financial losses to those who suffer from it, but also causing deaths. While the issue itself reached a point where full containment became impossible, we can work towards limiting the effects it has on people, moreover, Awareness must be made, especially to more vulnerable and less informed demographics. By decreasing the number of losses and consequently, proceeds to those who practice it, cybercrime may slowly but surely become a less sustainable activity, therefore, leading to a more cybercrime-free environment.

References

1. Apăvăloaie.E., The impact of the Internet on the business environment " (2015). ScienceDirect.
2. Bray, Jesse D., "Anonymity, Cybercrime, and the Connection to Cryptocurrency" (2016). Online Theses and Dissertations. 344. https://encompass.eku.edu/etd/344
3. CSOHomepage,https://www.csoonline.com/article/2124681/what-is-social-engineering.html. Last accessed 6 December 2021.
4. Proofpoint. (2019). Human Factor Report 2019 (Report No. 0819-032). Proofpoint, Inc.
5. Bertrand Russell (2013). "IIuman Society in Ethics and Politics", p.160, Routledge
6. Kevin D. Mitnick & William L. Simon.: "Controlling the Human Element of Security". The Art Of Deception, (2001)
7. CBS News, United States. Accessed 3 December 2021. <cbsnews.com/news/anonymous-hacker-hector-monsegur-turned-fbi-informant-breaks-silence>
8. Morgan, S. United States. Cybersecurity's Greatest Showman On Earth: Kevin Mitnick. Last accessed 1 December 2021. <https://cybersecurityventures.com/cybersecuritys-greatest-show-on-earth-kevin-mitnick/>
9. Linn F. Freedman.: "Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion". National Law Review, Volume X, Number 44 (2020)
10. FBI. (2020). 2019 Internet Crime Report. Federal Bureau of Investigation
11. FBI. (2021). 2020 Internet Crime Report. Federal Bureau of Investigation
12. Morgan, S. United States. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Last accessed 1 December 2021. <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>
13. Norton. (2017). 2017 Norton Cyber Security Insights Report Global Results. Norton by Symantec
14. FBI. (2021). 202 Elder Fraud Report. Federal Bureau of Investigation
15. Verizon. (2021). 2021 Data Breach Investigations Report. Verizon
16. Threat Intelligence. Threat Landscape Trends – Q1 2020. Last accessed 10 December 2021. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-q1-2020
17. Sectigo, https://sectigostore.com/blog/different-types-of-hackers-hats-explained/. Last accessed 6 December 2021.