jamk.fi

Social Engineering

Introduction to social engineering through real-life hacking attempts

Nina Helminen

Bachelor's thesis
May 2021
School of Technology
Information and communication technology

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Helminen, Nina	Bachelor's thesis	May 2021
		Language of publication: English
	Number of pages: 52	Permission for web publication: Yes

Title of publication

Social Engineering

Introduction to social engineering through real life hacking attempts

Degree programme

Information and communication technology

Supervisor(s)

Kokkonen Tero, Kotikoski Sampo

Assigned by

JAMK University of Applied Sciences / JYVSECTEC

Abstract

Social engineering is something that everyone is familiar in one way or another. We are dealing with it our everyday life without even noticing it. No matter if it is in work, holidays, or our home, where there are people there is social engineering. Social engineering is influencing someone to gain something to yourself. Usually this is used unnoticed, but it can be used in a malicious and criminal purposes also.

The task was to investigate what different kind of methods are used when using social engineering by influencing others and how it is used as a tool in cyber-attacks. In theory section the methods were inspected more deeply. The statistics were analyzed what attacks were used the most and how many attacks have been done compared to other years.

Some real cases of cyber-attacks in 21st century where social engineering was used were examined more closely. Analyzing the attacks should give more knowledge of what should be made different and how to avoid the situations in the future.

Some guidelines were added at the end of study of how oneself could be protected against social engineering attacks. The problem was how to notice when under attack and how to be protected against such attacks. Companies are playing a big role when cyber-attacks have risen toward them and has become one of the larges threats to companies. Education of employees has been one of the solutions and still is the cornerstone of cybersecurity. As said, humans are the weakest link and that is where the social engineering attacks are made to target.

Keywords/tags

Social Engineering, phishing, cybersecurity, penetration testing, impersonation, malware

Miscellaneous

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Helminen, Nina	Opinnäytetyö, AMK	Toukokuu 2021
	Sivumäärä 52	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty: Kyllä

Työn nimi
Social Engineering
Introduction to social engineering through real life hacking attempts

Tutkinto-ohjelma
Tieto- ja viestintätekniikka

Työn ohjaaja(t)
Kokkonen Tero, Kotikoski Sampo

Toimeksiantaja(t)
JAMK University of Applied Sciences / JYVSECTEC

Tiivistelmä

Social Engineering tai sosiaalinen vaikuttaminen on asia jonka kohtaamme jokapäiväisessä elämässämme. Törmäämme ilmiöön huomaamattamme, oli paikkana sitten työ, vapaa-aika tai koti. Sosiaalinen vaikuttaminen on vaikuttamista toisen käytökseen niin, että se palvelee omaa etua. Yleensä tälläinen käytös on harmitonta, mutta sitä voidaan käyttää myös rikollisiin tarkoitusperiin.

Työn tarkoituksena oli ottaa selvää eri keinoista joilla voidaan vaikuttaa toisiin ihmisiin sosiaalisen vaikuttamisen kautta ja miten sitä käytetään kyberhyökkäyksen välineenä. Teoriaosuudessa paneuduttiin eri keinovalikoimaan sekä tilastoihin, mitä hyökkäyksiä käytetään eniten ja miten ne ovat muuttuneet vuosien varrella. Lisäksi tutkittiin muutamia aitoja kyberhyökkäyksiä 2000-luvulta. Hyökkäysten analysoinnilla voitiin pohtia mitä olisi voitu tehdä toisin ja miten tulevaisuudessa vältyttäisiin vastaavanlaisilta hyökkäyksiltä.

Lopuksi tuotiin esille ajatuksia siitä, miten kukin voi itse suojata itseään kyberhyökkäyksiltä, mihin liittyy sosiaalista vaikuttamista sekä miten tunnistaa se. Yritysten näkökulmasta kyberhyökkäykset sosiaalisen vaikuttamisen keinoin ovat kasvussa ja yksi suurimmista uhista. Näin ollen omien työntekijöiden kouluttaminen uhkia vastaan on yksi tietoturvan kulmakivistä mihin yritysten tulisi panostaa.

Avainsanat
Sosiaalinen vaikuttaminen, kalastus sähköposti, tietoturva, penetraatiotestaus, imitointi, haittaohjelma

Muut tiedot

Contents

Figures

ABBREVIATIONS

COVID	Coronavirus disease
CVE	Common Vulnerabilities and Exposure
ENISA	European Union Agency for Cybersecurity
FINCSC	Finnish Cyber Security Certificate
IE	Internet Explorer
JAMK	JAMK University of Applied Sciences
LAN	Local Area Network
MITM	man-in-the-middle
OS	Operating System
PHEIC	Public Health Emergency of International Concern
PPE	Personal Protection Equipment
RegEx	Regular Expression
ROP	Return Oriented Programming
SE	Social Engineering
SIM	Subscriber Identity Module
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
WHO	World Health Organization
Wi-Fi	Wireless network connection

1 Introduction

Nowadays one can read many news about people who have been scammed through emails, and malware are implemented through e.g. a play store. Even enterprises have been giving money to hackers because they had impersonating someone else and have done it so genuinely that no one has guessed anything. These kinds of attacks are part of social engineering which this thesis is based on. Social engineering is a part of cybercrimes that can be used against people and enterprises. The thesis examines methods how people and enterprises are being scammed through web and the tools which make them possible to do so. In the end few real cases are examined more closely to find out how social enigneering has been used in real life.

Social engineering is often refferred to human hacking. When talking about computer security the weakest link is human. In social engineering goal is to target simply to human to make the error so after that, attack usually continues fast and far. Corporations try to educate personnel to avoid hacking attemps such as phishing which is the most common method to try to get direct access to the corporate data. There is also many training applications which can be in used inside corporate to keep employees alert because phishing attemps can be received even in daily basis.

Now in 2021 we are facing a pandemic which is causing people to seek information about something we have never faced before. This is causing people to be feared against something new and it is only natural. This is something that cyber criminals are taking advange of and in 2020 phising attacks spiked over 600% (Understanding and dealing with phishing 2020). This shows that people are more likely to be deceived when having motional influence to something that is close to us and in this case it is people´s health. Also the pandemic brought home offices and remote working. This has also be seen as a potential weak point to make more human errors more as in the workplace.

Social engineering is used part of attacks which main goal can be to get sensitive data and usually blackmail to gain personal profit with the data received. Sometimes the goal can be to bring some corporate down or at least make large damage. It really depends who is conducting the attack and what is the purpose of it. So no matter how small or big the attack is, in social engineering case it is always targeted to the people to make mistakes.

Jyväskylä Security Technology (JYVSECTEC) is JAMK University of Applied Sciences, Institute of Information Technology based research, development and training center focused for Cyber Security, Artificial Intelligence and Data Analytics. They offer services such as cyber exercises, training, testing, researching, consulting and Finnish Cyber Security Certificate (FINCSC) mechanism for companies. JYVSECTEC is operating part of JAMK Univeristy of Applied Science´s Information Technology and they are really close to students and their studies, helping and offering a thesis topics like in this case. (JYVSECTEC by jamk 2021) Social engineering is something that influences everyone´s life no matter if you are working or home. You can be targeted at any place and that said it is really important to be aware every possibilities how you can be scammed and how to avoid it. I am happy to be able to make this thesis to JYVSECTEC because social engineering is something that is happening now and it is not going anywhere.

Even if it might sound a bit scary that people can be scammed so many ways and unnoticed, that is not the reason to be overly afraid to use internet. There is ways to decrease the change to be targeted and in own behaviour and knowledge is to most important tool against social engineering attacks. Training and question the information received through internet can be most efficient tools a person can have against socail engineering attacks.

2 Research

2.1 Research question

This thesis strives to find the answer to the following research question:

- How people are being exploited using social engineering methods?

This is a main question that wraps around the essence of social engineering. While topic is quite large to go through in one thesis the main research question is qualified to the following sub-questions such as:

- How is social engineering used in 21st century by cybercriminals?
- What are the social engineering methods?
- How can one protect oneself against social engineering attacks?

Sub-questions should give some insight specifying the main question to the certain direction. Methodology of social engineering and practical guidance of protection against some attacks are questions that should narrow the social engineering topic a bit.

2.2 Research method

In this thesis the research method chosen to use was qualitative method. Qualitative means that the processes are not experimentally examined or measured in terms of quantity, amount, intensity or frequency. The qualitative method is designed to refer to studying real-world situations and study cases which are information rich and illuminative whereas the quantitative method uses measurements and statical information and analyses the data mathematically or numerically. The qualitative method can reflect the writer's own perspective as long as it has authenticity and is trustworthy. (Labaree, N.d.)

For this thesis the information used was found from different organizations such as World Health Organization (WHO) and TRAFICOM which are trustworthy authorities giving detailed information, recommendations and help how to perform when in need of help. The security companies offered quite useful info about the social engineering but keeping in mind that companies are marketing usually something so filtering the unrelated information is a must. Other thesis and blogs can be found useful and was used in thesis as a backing up some data found in different sources.

2.3 Research ethics

Research ethics should give guidelines of how to conduct a trustworthy research which is not violating the copyrights of any kind. To get the result of ethical thesis one must be honest when analyzing the data in hand. Keep the objectivity and not be influence the personal feelings of any kind as much as being careful when examining the data and thesis as full, avoiding any kind of errors and negligence. Respecting the intellectual property which means plagiarizing must be avoided in any cause. Honoring copyrights and giving the credit to whom it concerns in form of reference in text (Ethical Principles for JAMK 2018). These are the guidelines used when making this thesis. There is no reason for not to follow these principles.

3 Social Engineering

Social Engineering (SE) is based on influencing people by manipulation and deceiving. In this way it is possible to take advantage people to obtain information with or without the use of technology (Mitnick & Simon 2002). The attacker can use many tools to obtain the illegal access e.g., phone, emails, and even direct contact (What is social engineering? N.d.). The basis of social engineering attacks is to avoid the security systems by deceiving and exploiting the weakest link, people. The attacker who practices social engineering and is good at it usually knows how human mind works and how to manipulate it. (Barbosa, Breda & Morais 2017)

3.1 Categories

Social engineering can be divided in to two categories: Hunting and Farming. Main difference is the amount of interaction between the target and the attacker. Depending what kind of attack is used, it can be categorized one of the main groups.

Hunting

When hunting attacker try to have minimal interactions with the target. Once the security breach is completed and the objective achieved the communication is most likely to be drop and the victim never know that the attack took in place. This is the most used methodology to support cyber-attacks. (Barbosa, H. Breda, F. Morais, T. 2017)

Farming

Farming is not as common as hunting, but it may come in handy in some situations. When farming, attacker needs to establish a relationship to the victim to “farm” information. This may include bribery or threating if the needed information is required. (Barbosa, Breda & Morais 2017)

3.2 Phases

We can separate Social Engineering in to four different phases according to Salahdine and Kaabouch as illustrated in Figure 1.

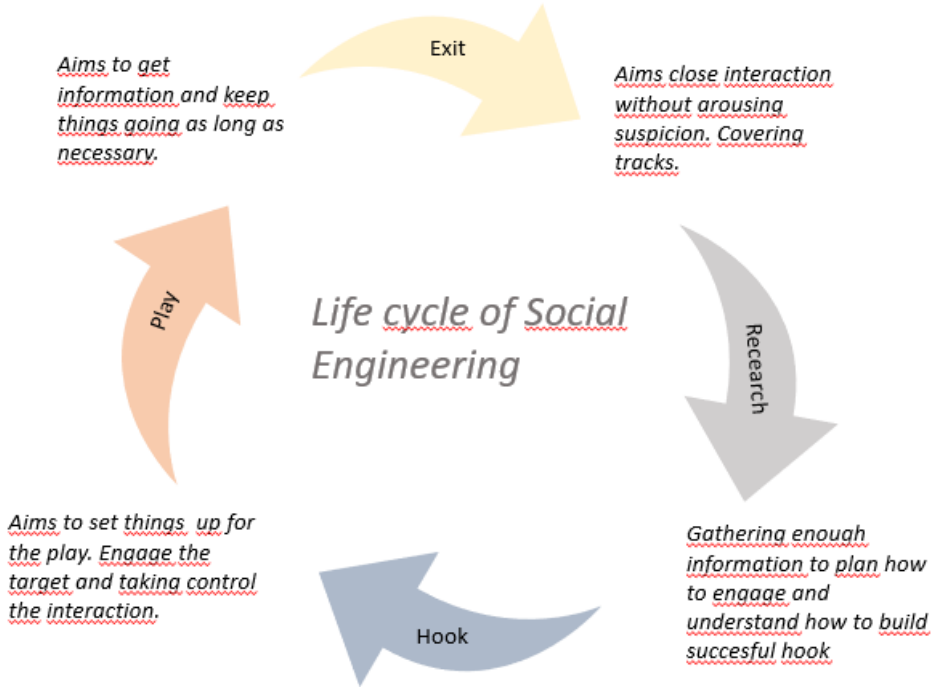

Figure 1 Social engineering phases (McAfee Labs 2015)

Research phase

When gathering information, the internet is the best place to look for it. One can easily find peoples´ profiles in Facebook, LinkedIn, Tinder, Twitter, Instagram with pictures and personal information such as jobs, educations, family, friends and much more. Attackers usually make fake profiles and gather information by inviting people to be friends and then mine the information. (Salahdine & Kaabouch, 2019) If gaining the right information, it is possible to determine what attack vector to use, possible passwords, individuals' responses and to refine goals (The Social Engineering Framework 2021).

Hooking to the victim

When the needed information has been gathered, attacker can try to establish a relationship to a target. Usually this takes place by adding him/her as a friend and starting to gain some trust. It can take some time; however depending on the value of the attack the result may be worthwhile (Salahdine & Kaabouch 2019). Contact to the victim can be as much as a brief smile and eye contact as attacker hurries through door or it could be a phone call or even sharing a family pictures with the receptionist (The Social Engineering Framework 2021).

Playing phase

This is a phase when the victim is played by the attacker to make a security mistake or give out sensitive information for example about the passwords. When the needed information is gained the attacker can execute needed actions. (Salahdine & Kaabouch 2019) The tools to use in this phase can found on the internet and in instructional videos showing how to use them. Usually, the tools are made for educational purposes only but if someone has bad intensions one is solely responsible for them.

Out and fast

In the out/exit phase the attacker leaves the scene without any proofs or trails that he/she ever existed. This would be the preferred situation for the attacker. (Salahdine & Kaabouch, 2019)

3.3 Social Engineering statistics

The last ten years the threat of social engineering attacks has been increasing. The exploits have been evolved as the threat actors has been moved to the digital landscape. There are new tactics and targets which makes the attack volume to rise every year. (2019 Phishing trends – N.d.). According to Purplesec security report in 2019, 98% of cyberattacks has some form of social engineering during 2018. The same report mentions that 21% of employees, current or former, use social engineering for a

revenge or gaining the financial benefits from the company. The phishing attacks e.g., targeted emails, spear phishing, has been used in 91% of successful data breaches and 95% of all enterprise networks. By the end of 2017, an average user received approximately 16 phishing emails a month. It has been predicted that in 2020 money spent on cyber security will reach in 1 Trillion dollars (The Ultimate List of Cyber Security Statistics For 2019. N.d.). In Figure 2 shows what are the most common attachment types e.g., in emails that spreads malware to the victim in 2018. Figure 3 illustrates that the common distribution ways that the malware is delivered to the victim in 2018 was through invoices and bills. Emails was a close second and after 2018 the portion of email attacks has only risen as seen in Figure 4.

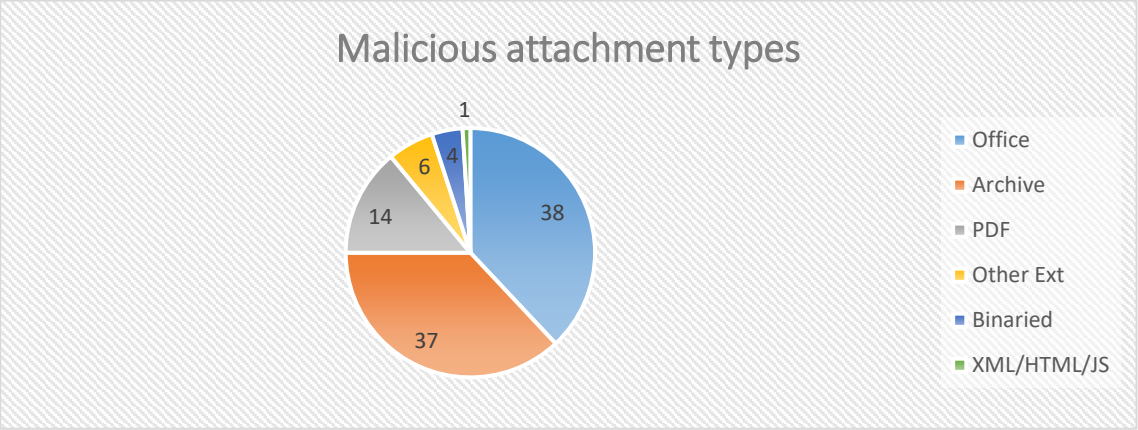

Figure 2 Most common malicious attachment types (The Ultimate List of Cyber Security Statistics For 2019. N.d.)

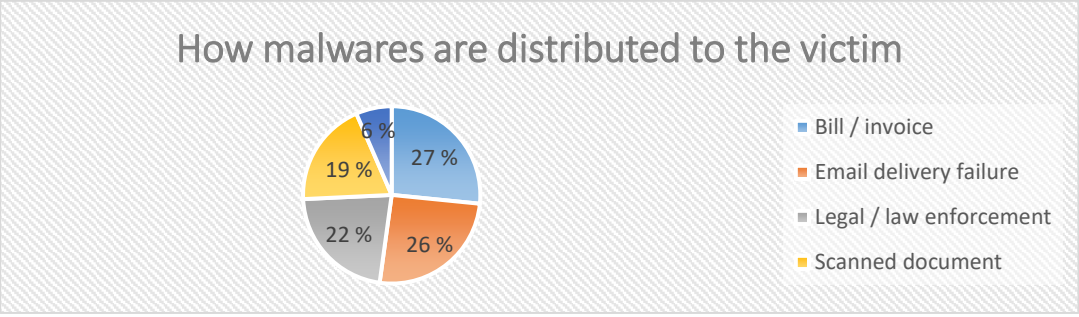

Figure 3 How malwares are distributed to the target (The Ultimate List of Cyber Security Statistics For 2019. N.d.)

The statistics shows that the desktops and laptops are the most vulnerable to attacks as well as smartphones (Figure 4). Emails are the most used when trying to implement malwares to the device. Trojans are leading form of malware when speaking Android operating systems. These shows that email is the most common threat in over 90% case, and it should be taken seriously. Cyber-attacks through social actions use emails in 96% of time and in 2019 and 9.2 million users did report to receiving a suspicious email and 29% of them did open the phishing email. 46% of organizations got malicious email where 5% data breaches were caused by compromised organization emails (73 Important Cybercrime Statistics 2021).

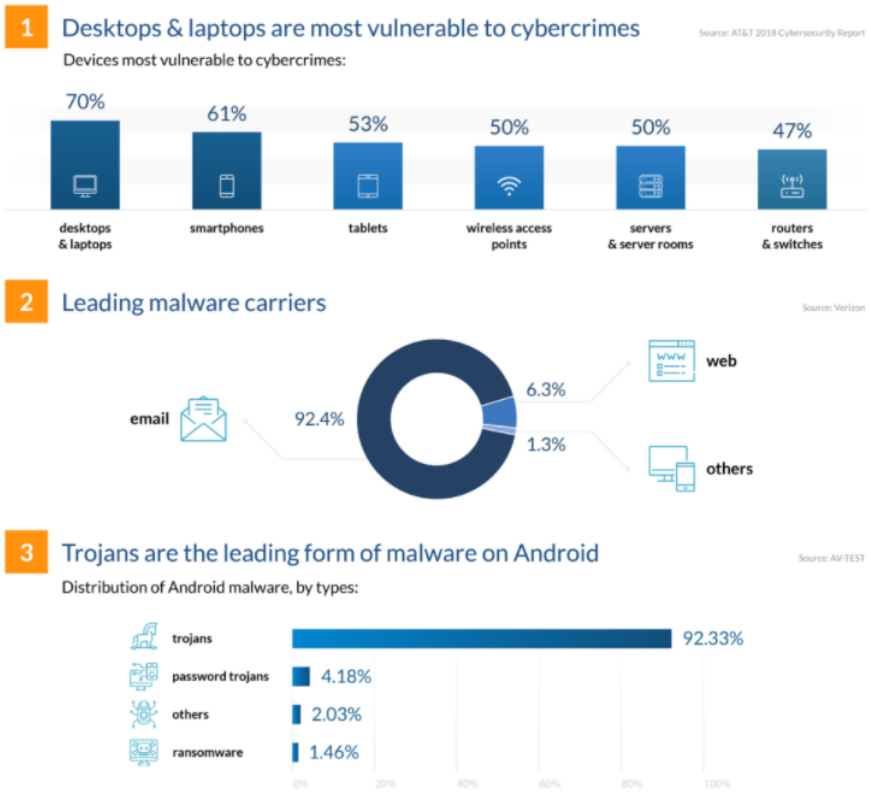

Figure 4 Key statistics from 2020 (73 Important Cybercrime Statistics 2021)

4 Tools

Penetration testing tools

Penetration testing, also known as pentesting is used in testing an organization's cybersecurity vulnerabilities. With penetration testing it is possible to view a network, applications, devices, and physical security and discover possible weaknesses and identify possible areas to improve the security. (Talamantes N.d.)

There are different kinds of penetration testing tools that can be used in social engineering. They are divided into three different section, socio-technical tools, physical tools, and social tools. Usually, to make successful attack one needs to implement the malware using either socio-technical tools, physical tools, social tools or all of them depending on the style of the attack is being made. Some of the most used tools used in social engineering attacks are discussed below.

4.1 Socio-Technical tools

With social-technical tools, the attack can be made from distance. Usually, the attacker is using IT equipment to scam or bait victims to fall into trap. With such tools it is possible to take over someone´s account and from there it is possible to start another attack like lateral phishing.

4.1.1 Phishing

Phishing is a method where an attacker is trying to fraud as many people as possible, for example using phishing emails. From phishing emails, it is possible to obtain users´ usernames, passwords and even bank account details. Phishing is targeted at a large group of people and it is counting on that someone is going to fall for it, which is enough. If one is using voice over internet protocol (VoIP), the phishing is called vishing and if using short message service (SMS), it is called smishing. (Verkkourkinta N.d.)

Mechanism

Social fish is one of the tools that KALI and Black Arch offers for phishing over known services such as Facebook, Twitter, and Instagram. It can be downloaded from GitHub repository *https://github.com/UndeadSec/SocialFish* but Black Arch, which were used for experimentation showed in Appendix 1, they had it already in the default tools. There are many similar tools e.g., HiddenEye, BlackEye and phishX. Some tools can create a poll which can be effective to get people to answer them and then one needs to sign in the social media page to share the result and of course the sign on page is fake. However, with Socialfish one needs to get the people to click the link for example from scam e-mails. All these tools are used own responsibility and they should not be used in illegal purposes.

4.1.2 Spear phishing

In Spear phishing the attacker is targeting a specific target, which is the difference from regular phishing. The target is usually someone inside at corporate or government. In spear phishing the attacker is trying to get the information about the target through social engineering. The method used in spear phishing is the same as in normal phishing; hence the victim is lured to click on a malicious link or attachment or even visit malicious website to get the information needed. (Phishing/Spear phishing N.d, Spear Phishing Attack N.d.)

Mechanism

When using spear phishing, the attacker needs to know something about the victim. The information today is easy to obtain through social media. Spear phishing is usually the method when trying to penetrate company´s defenses and make the real attack. According to SANS institute 95% of network attacks in enterprises are successful when using spear phishing. (What Is Phishing? N.d.) Then the attack is made similarly as in phishing but targeting the wanted victim. The targeting can take place by sending a malicious email or message through social media to the right person.

4.1.3 Lateral phishing

Lateral phishing is targeted to the actual victim´s friends or contacts. This is an effective because the malicious link or attached file is coming from someone familiar and it is trusted more easily (Barry 2020).

Mechanism

Lateral phishing is an internal attack which means that email security gateway cannot detect the attack. Usually, phishing is made with spoofed or external accounts so lateral phishing can be hard to detect. According to Christine Barry, Senior Chief Blogger and Social Media Manager at Barracuda security company, roughly 11 percent of lateral phishing has been successful to compromise more accounts which can lead to a more lateral phishing attack. (Barry 2020, Lateral Phishing N.d)

Lateral phishing attack starts when account has been already taken over. From there it is quite easy to send emails to the contacts that are known from the stolen account. This can be quite harmful when thinking about companies' point of view. It can affect all the employees and even external organizations. With the lateral phishing it is possible to gain more information about the organizations, employees or even spread malicious content to inside the company (Lateral Phishing N.d).

4.1.4 Whaling

Whaling is almost the same thing than spear phishing; however, it targets high-ranking individuals or enterprises. That is the reason a whale is used to describe a big target but the method that is used is still phishing. (Whaling attack N.d.)

Mechanism

When whaling, the attacker needs more social engineering skills to find high-ranking target´s contact information. Planning is more important because one could think that going higher in rankings would mean that the protections can be more secure. The attack is carried out in the same ways as phishing; e.g. the content of malicious

email should contain personalized information, it often is urgent and crafted in business language so that it is hard to separate from the right emails (Whaling attack N.d.).

There has been a new trend in whaling where it is combined with a phone call. This social engineering tactic can be described as *cyber enabled fraud*. It uses the trust of the partnership against the target. The attacker sends malicious email and then calls and masquerades him/herself as a partner who just sent the email and wants to make sure that the email has arrived, and it could be urgent. This gives a sense of trust to the victim that the email can be real and not cyber-attack because of the "real world" interaction. (What is whaling attack (whaling phishing)? N.d.) Combining attacks will give higher success rate and social engineering is mostly use part of the bigger attack.

4.1.5 Watering hole attack

Watering hole attack is advanced social engineering attack which requires good technical knowledge from attacker. In this attack the attacker identifies websites victim often uses. When the websites are chosen by the attacker, she/he infect the website and just wait the victim to visit the site and fall in to trap. (Barbosa, H. Breda, F. Morais, T. 2017)

4.2 Physical tools

Physical tools are gadgets that need to be implemented into a victim´s personal space. It can be directly attached to the victim´s computer or inside the enterprise. Using social engineering to make oneself disappear in the crowd can be a useful skill. To make oneself someone else face to face can be more difficult than pretending to be someone else over the internet. It needs more planning and even fake identifications if the attack requires implementing something malicious inside the computer or company. Physical tools were found in company called HAK5, which makes

penetration testing tools for administrators and for security personnel. These gadgets can be used in malicious purposes as well, which is why physical tools are included in this thesis.

4.2.1 Rubber Ducky

Rubber Ducky is USB drive where one can install backdoors, steal passwords, execute different penetration test tasks and script it to do so much more (Hak5 N.d.a). The attacker needs to get in-to a victim´s computer imperceptibly and here the social engineering can come handy.

4.2.2 LAN Turtle

LAN turtle looks like an USB Ethernet Adapter, but it can be used in the man-in-the-middle attack to gain remote access, gather some information from network intelligence. It is undetectable when blending in into an IT environment. The LAN turtle can come with 3G where one can put one´s SIM card and get one´s own internet connection. With this it is possible to get reverse shell or even VPN endpoint and bypass the firewall. (Hak5 N.d.b) This is also needed to implement inside the corporation. In Figure 5 is shown how easily a little device looks like a normal USB Adapter and can get unnoticed by user.

Figure 5 LAN Turtle (Hak5 N.d.)

4.2.3 WiFi Pineapple

WiFi Pineapple is a rogue access point which can be used for example in man-in-the-middle attacks, credential harvesting and network traffic analyzing. (Hak5 N.d.c) It is like other physical tools used in attack purpose; one needs to get close to victim, inside the enterprise or victim´s house, so the Pineapple is in the network range to

make itself the rogue AP. The WiFi Pineapple will clone the other network names and when the connection is made the victim thinks it his/her own network; however, it connects to the Pineapple first, which makes the man-in-the-middle (MITM) attack. The traffic then goes through the victim to the Pineapple which is the attacker´s device and she/he can get all the information she/he wants there. The traffic goes after that normally to the internet without the victim noticing anything weird (Hakkarainen 2020). It is notable that WiFi access points are just like the Pineapple, only weaker. This means that the Pineapple has multiple radios comparing to the only one which normal routers have. That is why Pineapple can interface hundreds of devices at the same time (Oberhaus 2017).

4.3 Social tools

With social tools it is possible to fraud people without any IT equipment. The method allows attacker to gain information at close distance. Usually, attack can start with social tools such as eavesdropping something useful what you can use when making the bigger or rest of the attack what has been planned. Socio-technical tools and social tools are often used together when making an attack.

4.3.1 Tailgating

Tailgating means following someone to a restricted area or system. This needs the impersonation at its best and some props to pull this off, e.g., costume or package to deliver or anything that gives a reason to go to a restricted area. (Phishing/Spear Phishing N.d.) Nowadays when the smoking is prohibited indoors one of the increasingly effective technique is to tailgate group of smokers inside to the building (Barbosa, Breda & Morais 2017).

4.3.2 Impersonation

Impersonating someone can be a useful skill to trick people. One might be able to get passwords through phone impersonating to be from IT department or even get to someone´s computer for a fake identification. It is the human nature to believe someone with authority or credentials such as badges and identifications or even a uniform of delivery service or security. (Social Engineering: Impersonation 2016). The main issue is to have the trust of the victim in one way or another. Common techniques where impersonating is needed to trick people are piggybacking, pretexting and quid pro quo (Barbosa, Breda & Morais 2017).

Piggybacking

Piggybacking can be compared to tailgating. It is used in same manner as in getting to the restricted area. But in piggybacking the objective is to gain legitimate access by using impersonation such as IT-support who needs temporary admittance to the area. (Barbosa, Breda & Morais 2017)

Pretexting

Pretexting occurs when someone is claiming to be an IT employee and asking an employee to give credentials (password and username, identification) or log in to the wanted device for maintenance purposes. (Phishing/Spear Phishing N.d.)

Quid pro quo

Quid pro quo means “something for something”, which is like an exchange for something. For example, the attacker offers some money and in exchange wants to have the password. This can include a background story why the money is offered for e.g. research purposes. (Phishing/Spear Phishing N.d.)

4.3.3 Baiting

Baiting may be done without impersonation but in some case, it can be needed. For baiting attacker needs to lure victim for example put an USB drive to the computer.

The USB drive contains malicious code or malicious files that when opened can give access for the attacker to penetrate the computer. The USB drive can be only lying around somewhere and as curious as people can be, someone usually wants to see what is inside. (Phishing/Spear Phishing N.d.)

4.3.4 Eavesdropping

Just being at the right place at the right time, it is possible to hear classified matters from the authorized personnel if speaking out loud. Also listening other communication channels such as telephone lines and e-mails are count as eavesdropping. (Barbosa, Breda & Morais 2017)

4.3.5 Shoulder surfing

Shoulder surfing is to peak victim´s shoulder to collect personal information, usually authentication data. (Barbosa, Breda & Morais 2017) Shoulder surfing can be made almost any situations where there are people around. That is why any confidential information should be only viewed in the secured area.

4.3.6 Dumpster diving

If organization have adequate disposal of sensitive information, dumpster diving can come handy. The attacker simply goes through organization´s garbage in hope to find the information what can be used in attack. (Barbosa, Breda & Morais 2017) Companies and organizations should have secure disposal for a sensitive data because the data might also concern sub-contractors as put them are also vulnerable to attacks.

4.3.7 Reverse social engineering

In reverse social engineering attacker creates a problem and then acts as a solving person. When help is needed, he/she presents a solution to the problem he/she created (Barbosa, Breda & Morais 2017). In this way the suspicious is minimize and attacker can solve the problem or just wait until he is contacted by the victim depending on the attack.

5 How to protect yourself

Knowing how to protect yourself from phishing or how to make you less desirable target is the most important thing to know against social engineering attacks. As said social engineering goal is to target people and getting the information needed one way or another. There is a different way to protect property depending on is it organization what needs to be protected or an individual. Even if the ways are similar the behavior varies.

5.1 Individuals

As in individuals, it is important to secure own network. The main goal as an attacker is to gain something and it is usually money and information / data which in worst case of scenarios can lead to an identity theft. The easiest way to gain something is phishing as said earlier. E-mail phishing can be made good that it is impossible to notice it. That is why it is important to know what information is really needed if you are logging webpages. One good advice is to now click any link what you don´t know or think it might be suspicious. Good example is to get some email from bank and there is a link to bank´s page. The message can be something simple like “you have one message, and you can read it from link below.” In this case you can always type the domain name yourself and it is a secure way without clicking any links and check if the message really is there. Always, if there is another way to go somewhere in secure pages without pressing suspicious links, it should be used. Also, it should be widely known that no authorities are asking any personal information via emails. In email phishing especially in Finland there can be a lot of grammar errors. If the message has grammar errors, there should be some doubts if the email is real. (Understanding 2020, TRAFICOM 2019)

Another bad habit is to have simple passwords. In nowadays people have so many services to logging and many users use same passwords over again. And if that is not

enough it usually is easy to guess. This can make many accounts in danger if one is hacked. There is easy solution to protect your accounts, hard passwords and/or 2-way authentication if available (TRAFICOM 2019). It is possible to use password managers like KeePass where you can choose randomly made strong password and save it in the database. It is easy to use, and you don´t have to remember every password in every account.

In every gadget and devices which has access to the internet should be updated and have some sort of anti-virus and anti-spyware protection. Usually there is possible to choose automatic update so you don´t even have to remember to update your devices but time to time it should be checked that everything is up to date. (Understanding 2020, TRAFICOM 2019)

5.2 Organizations

In organizations there is usually lot in stake. There is more money going and sensitive data in corporate worlds that in wrong hands can cause lots of harm. Most of the ways are the same as listed previous chapter. Employees should always be wary when receiving corporate emails. The same instructions apply here as in never give any sensitive information via emails and look grammar errors or suspicious links or attachments. Updates should be checked in regular basis if employee has a personal computer.

In corporate world the target can be specified. Whaling is used more often to catch the big fish. In a single company can have subcontractors which increases the risk of getting cyberattacked. The security should be designed properly where everyone knows their responsibilities and how to act when having incidents. Criminal's goal can be to target the third party to gain access to the main company by stealing access rights, so this is something to think about. (TRAFICOM 2019)

Training your personnel is something that many companies nowadays have. There can be even some cybersecurity training programs like. HoxHunt platform is made for employees to recognize phishing attempts and to report them. If the attempt is a “fake” the employee get stars and program tells what was wrong in that email. If suspecting a real phishing attempt it can be report through the platform. (Phishing awareness training that employees love 2021)

Something that every company should do is to have a backup and even backup´s backup. There have been cases that even the backup has been encrypted by the hackers in ransomware attack and that can be situation that is hard to prepare if not thinking it really might just happen. There is something called “3-2-1” -method that is good way to storing data. The method is to have three recent copied of the date to store two different locations and to one cloud storage provider. In this way the data should be recovered in the case of cyberattack. (Infosecurity 2020)

5.3 In case of getting hacked

If there is even a slight chance that person finds that she/he has is a victim of phishing, there should be some precautions to make. First, if any malicious link or attachment has been opened or downloaded the security scan should be made. Checking all the updates of anti-virus and anti-spyware programs and scanning the whole computer. After that all the logging credentials should be changed specially if the password is same in many services. If there is a bank involved, contact bank, or credit card company and explain what has happened. (Understanding and dealing with phishing 2020)

As in corporate employee, inform immediately to the IT department and follow their instructions, usually forwarding the malicious email so to IT or security department for further investigation; it shouldn´t be deleted before that. Notifying that organization has been spoofed is crucial so that everyone is aware of but who is giving the

information of incident depends on company´s strategy. (Understanding and dealing with phishing 2020)

6 Real cases

6.1 What really can happen

I wanted to introduce some of the real cases where social engineering attacks has been used. The last one concerning pandemic came during making this thesis. This only tells that cyber-attacks are happening all the time especially when something sudden happens. Real cases were easy to find but hard to investigate. Hopefully these cases can point that no one is safe from attacks not even big corporations nor individuals.

6.2 Ubiquiti Networks Inc.

Ubiquiti Networks Inc is an American network technology company. They provide wireless and wired technology platforms for customers. The company was founded in 2005 by former Apple engineer Robert Pera and it has a global customer base. (Spear Phishing: Real Life Examples 2016, Work at Ubiquiti! N.d.)

In June 2015, the company had a spear phishing attack which cost them $46.7 million. The attack was made by using employee impersonation and fake request from outside in order to target the company´s finance department. The fake request, spoofed email, was targeted at Ubiquiti employees to make them think that the request was a legitimate request from the company´s director. It had look-alike domains and a spoofed email address, so it was easy to trick victims to finish the attack. The attack purpose was to transfer money from the company´s subsidiary incorporated in Hong Kong to overseas accounts. The Ubiquitin's employees made the transfer thinking it was legitimate which it eventually was not. (Spear Phishing 2016)

6.3 Dyre banking Malware

Dyre/Dyreza banking malware is a phishing campaign which has been going on since mid-October 2014. It has been changed slightly to, make it easier to lure people to reveal their banking details. This phishing campaign has many elements such as attachments, exploits, themes, and payloads. The main purpose remains the same as in phishing overall, to trick victim to open malicious attachment or download the malware. Malware is carried by spam emails where the malicious attachment is, as seen in Figure 6, or a malicious URL where the victim is tricked to browse. Dyre can also be used to create botnets which are used to infect other computers. It targets Windows computers and most used browsers such as Chrome, Firefox, and Internet Explorer. Dyre malware often uses a PDF attachment because the exploit found in unpatched Adobe Reader versions. (Dyre N.d, Phishing Campaign Linked with 'Dyre' Banking Malware 2014).

The vulnerabilities found in Adobe Reader was CVE-2013-2729 and CVE-2010-0188. The Common Vulnerabilities and Exposure (CVE) is a list of entries which each has an identification number and description. In this case the Adobe had the attackers targeted at CVE-2013-2729 and CVE-2010-0188. The CVE-2013-2729 was targeting the Adobe Reader and Acrobat versions 9.x before 9.5.5, 10x before 10.1.7 and 11.x before 11.0.03. These versions allowed the integer overflow which allowed attackers to execute arbitrary code. The CVE-2010-0188 was concerning Adobe Reader and Acrobat versions 8.x before 8.2.1 and 9.x before 9.3.1 which also made the arbitrary code execution possible but also could cause denial of service and led the application to crash. (US-CERT Warns Dyre Malware 2020, CVE Common Vulnerabilities and Exposure 2020a, CVE Common Vulnerabilities and Exposure 2020b, NATIONAL VULNERABILITY DATABASE 2017).

It was reported in November 2015 that Dyre has evolved to support Windows 10 and Windows Edge browser. It has become one of the most startling modern-day banking Trojans. There have been some clues that the malware could come from Russia

because the Dyre spam campaigns were inactive at the time when Russian hackers were reported arrested. (Dyre N.d, Phishing Campaign Linked with 'Dyre' Banking Malware 2014.)

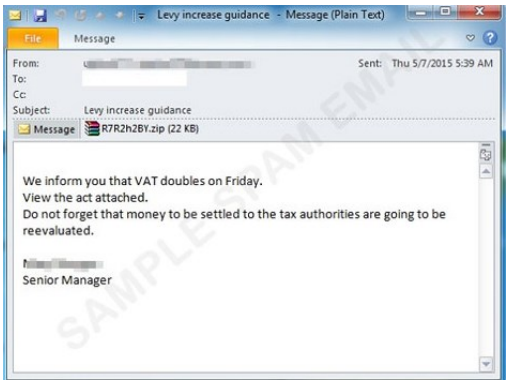

Figure 6 Spam email with malicious ZIP attachment (Dyre banking Trojan infections more than doubled 2015)

The one of the new variants of Dyre is called the Dyre Wolf. It appeared in 2015 when it started to support Windows 10. The difference in the old Dyre is that the new variant is programmed to monitor online banking sites and this way it can launch a spoofed page when a user logs into his bank account. The site gives an error message about an issue, and the user needs to call a number provided with the error message. Once the call is made, the user and in this case the victim is tricked to reveal his/her credentials for whatever reason. (Kitten 2015) It is all in the imagination of the attacker to invent some believable story behind the reason.

6.4 Forbes.com

Forbes origins United States and has been founded in 1917. It is a media and publishing company which provides daily news, sports, technology, business and the best-known list of ranking billionaires under age 30 (What is Forbes 2021).

Back in 2015 Forbes.com spokesman Laura Daunis made a statement that Forbes.com had an incident on November 28th in 2014 and it was identified few days later first of December (Hackers infect Forbes.com 2015).

It has been suspected that the Chinese hacker group was behind the attack and one of the reasons were that the malware was written in simplified Chinese. The malware was in Adobe Flash widget. The widget´s purpose was to take visitor to Thought of the Day page when visiting Forbes.com. Only targeted victims were taken to the malicious site where the exploit would happen. There was a zero-day vulnerability in Adobe Flash what was used using the exploit and in Internet Explorer (IE). Anyone using Windows operating system above XP or different browser than Internet Explorer was safe from the attack. Malware was designed to search victim system information and after downloaded it to the target´s system. (Forbes.com Hacked In November 2015)

In Figure 7 there can be seen how the attack proceeds when it is triggered by the victim. The attack is supposed to start when the malware recognizes the victim´s operating system. If the operating system is XP or below it will continue to recognize the browser what was used when entering the Forbes.com. If the browser is not IE or Firefox and if the Adobe Flash player is not in use, the exploit is aborted. But if the browser is the “right” one the malware continues to build ROP chain. ROP chain is a Return Oriented Programming which allows attacker to execute their own malicious code (ROP Chain 2017). After ROP chain attacker can try to make the successful exploit. If the XP is not recognized in the start of the exploit it will try to go for the secondary attack vector which is the IE. If it is not recognized the exploit will abort. But if the exploit will go to so call RegEx InfoLeak, where RegEx means Regular Expressions, it will continue build ROP chain and try the exploit. RegEx InfoLeak is used to leaking information from victim’s sensitive data. RegEx can also be used to find sensitive data matching the data against patterns (Using Regex to Find Sensitive Data N.d).

After Forbes found out the incident, they run different virus scanners like Virus Total. They found out that there were related malwares wuservice.dll and Wuservice.dll which were trying to get the foothold on victim´s machines and getting the needed information. Although not all antivirus vendors were able to identify the malware but some of them were able to block it. Microsoft patched the IE´s vulnerability as did Adobe for his Flash. The conclusions were that any of successful exploitation was not reported and as far Forbes is saying no foothold on Forbes´ network was established. (Forbes.com Hacked In November 2015)

The vulnerability of Adobe Flash was patched as CVE-2014-9163:

> *"Stack-based buffer overflow in Adobe Flash Player before 13.0.0.259 and 14.x and 15.x before 15.0.0.246 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in December 2014."*
>
> *(CVE N.d.)*

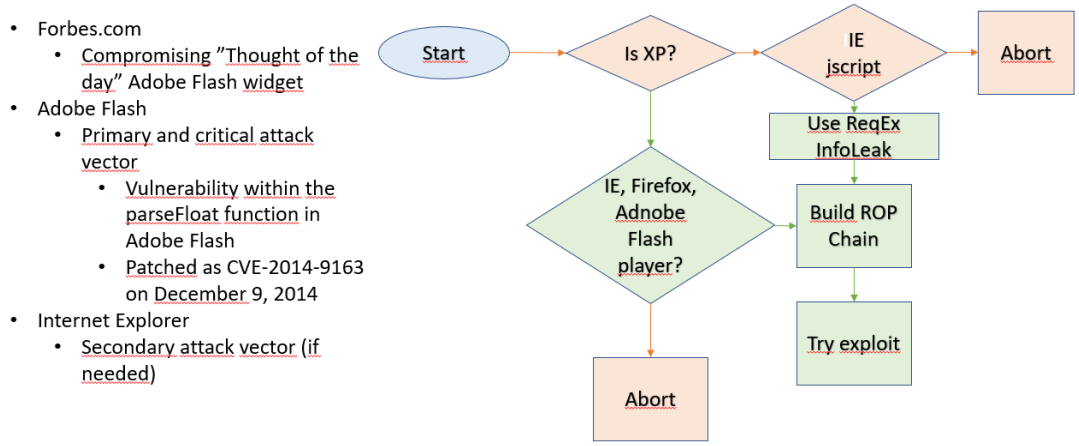

Figure 7 Forbes.com Watering hole attack (Forbes.com Hacked In November 2015)

6.5 Corona virus

During this thesis we have on going pandemic caused by Covid-19. The reason I am bringing this up is because the outbreak made the cybercrimes rise considerably and Covid-19 has been said to be one of the largest cybersecurity threats. (43 COVID-19 Cybersecurity Statistics 2020). Since the outbreak happened phishing has been reported to increase by 600% in March 2020. During April 2020 Google was blocking 18 million malware and phishing emails daily related to the virus (Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple & Bellekens 2020).

Corona virus (COVID-19) is a virus allegedly originated China. It has been spreading all over the world ending up being pandemic in year 2020. It has caused people to seek information because this disease is unknown, and the information is therefore limited (Finnish institute for health and welfare 2020). The attackers are taking advantage of people´s fear and anxiety of the newly recognized virus. Attackers has been reported to impersonating healthcare organizations and public authorities sending emails regarding to the COVID-19, making fake applications and informational websites to lure unsuspected users to fall into trap or even to dress up health advisories to infiltration of people personal space. The time that people is working at home because the quarantine, there is more opportunities of social engineering attacks (Ropek 2020).

World Health Organization (WHO) is the main organization fighting against the COVID-19. It is known trustworthy source of information and they have been giving the updated information during the outbreak of virus. This is the opportunity to the criminals to disguising themselves as a part of WHO and sending phishing emails. The emails usually contain requests of sensitive information, luring to click a malicious link or to open a malicious attachment. These are the methods criminals are using to steal sensitive information using phishing and the fear of COVID-19. WHO are giving information to deal with these kinds of scams in their website and how to verify the authenticity of communication because it is know that the attack can happen also

through phone calls, text messages and fax messages (World Health Organization 2020).

The Finnish cybersecurity center are informing people also for the phishing scam. In these scams, criminals are impersonating someone else and are trying to sell breathing masks. The victim ordering these products get nothing in return for his/her money.

Another scam is related to the John Hopkins university map. The map´s purpose is to track the Global Cases of COVID-19. The fake interactive maps can steal users' passwords, usernames, credit card numbers and other information used in browser sessions. How to prevent these kinds of scams is to find the information and related maps and others related apps from the trusted sites directly (TRAFICOM 2020). Of course, making things a bit difficult even more, cyber-criminals has been increasing the success rate of phishing scams by identifying large numbers of website domains such as *Corona-virusapps.com* and *anticovid19-pharmacy.com*. Domains containing words like corona and coronavirus paired with reputable wording such as pharmacy like in the example *anticovid19-pharmacy.com* can be thought as a trusted site but in this case it is not. (Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple & Bellekens 2020)

6.5.1 Covid-19 background

In the end of 2019 WHO office in China was informed that there were cases of pneumonia of unknow etiology found in Wuhan City, Hubei province of China. It was suspected that the cause of the pneumonia was in food market which was closed on 1st of January 2020 for the sanitation and disinfection of the environment (Pneumonia of unknown cause -China 2020).

In the timeline 31.12.2019 – 5.1.2020 there were 59 cases of pneumonia in Wuhan and the Chinese authorities informed that it was a new coronavirus that was causing

the pneumonia symptoms to the patients (Kiinassa todetut keuhkokuumetapaukset 2020).

This was the time that people were not worried so much about the new virus. It was only in China and there were not any cases outside of Wuhan until 31.1.2020 when WHO announced that the virus was an international threat or as in Public Health Emergency of International Concern, PHEIC (WHO julisti koronaviruksen 2020). Because the Covid-19 was spreading fast and there was no sign slowing down WHO had to announce Covid-19 as a pandemic on 11th of March in 2020 (Rolling updates on coronavirus disease (COVID-19 Cybersecurity Statistics 2020).

Covid-19 spreads from person to person through direct contact and have alike symptoms that regular flu so that is why it has been spreading so quickly and all over the world. Even if the Covid-19 is like the flu it is a more serious infection. it has been diagnosed that around 20%-30% of COVID-19 cases are hospitalized and 2% of those have severe illness. The Covid-19 can be fatal to the older people and for others who may have underlaying health conditions. (Q & A on COVID-19: Basic facts 2020)

6.5.2 People and Covid-19

So how this virus is related to the cybercrimes. When there are any signs of weakens seen in people there is those who want to exploit that. And Covid-19 was no difference. Covid-19 brought up the fear and anxiety in people because it was something new, and it was going to influence all the people in the world. People were gathering as much information as they could possibly get, and cybercriminals saw their moment to come. When people moved to working from home it was a new opportunity to cyber criminals as much as a new challenge for industry to prevent and protect the companies from cyber-attacks.

Cyber-attacks were not only influencing individuals but also, they were targeting critical infrastructure such as health care services and governments. In September there

was a cyber-attack into the hospital in Germany and the worst scenario happened, a patient died. Even if the attack wasn´t directed to the hospital but to the university near the hospital, attackers didn´t realize that the hospitals database was a part of the infrastructure, so it affected it also. With this remorse the attackers restored and cancelled the demands of the locked files, but they are still accused of murder of one people. (Hakkereilla on käsissään verta 2020)

This attack apparently was an accident and many of the cyber criminals are leaving hospitals and companies that are developing cures to the Covid-19 alone. Mikko Hyppönen who is a security and privacy expert in F-secure made an appeal to the cyber-criminals in his twitter account on March 18th of 2020:

> *"Public message to ransomware gangs: Stay the f away from medical organizations. If you target hospital computer systems during the pandemic, we will use all of our resources to hunt you down."*
> *(Hyppönen, Mikko, @Mikko)*

This had a small impact and at least one ransomware group called Maze announced that they won´t be making any attacks to healthcare organizations (Abrams & Lawrence 2020).

6.5.3 Cyber-attacks

In the Figure 8 there is seen in the early 2020 how the cyber criminals can response to the current event needed and how fast it can be in United Kingdom. For example, 25th of March in 2020 the UK government announced intention to make home testing kits for Covid-19 available. Just 6 days later there is a phishing campaign to lead victims to a fake website which are selling fake Personal Protection Equipment (PPE).

In the analysis made by Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple & Bellekens in 2020 the phishing (including smishing) was the most common attack, and it

was involved in 86% of global attacks. This is mainly because phishing is low cost, high success rate attack and you can easily perform it to a large group.

Event date	Event	Incident date & type	Incident
21-02-20, 09-03-20	Doctors warn GPs are running out of PPE; Hospitals running out of PPE	17-04-20 p, ph, f 27-05-20 p, ph, f	Fake PPE offers through email. Link to URLs which capture credit card and other details
11-03-20	Government announces a range of financial assistance packages in the budget	20-03-20 p, ph, f	Smishing campaign promising a COVID-19 financial relief payment. Respondents are directed to a fake *gov.uk* website which requests credit/debit card details
19-03-20	Government announces a scheme which entitles children who qualify for a free school meal to a food voucher or alternatives if they are not able to continue attending school.	24-03-20 p, ph, f	A smishing campaign which targeted parents with a promise of help with their free school meals in return for banking details. Banking details are defrauded
23-03-20	Lockdown announced. £60 contravention fine, later (10-05-20) increased to £100	27-03-20 p, e	Lockdown contravention SMS
24-03-20	COVID-19 hardship fund enables councils to reduce council tax bills by £150 for residents of working age and who have had their bill reduced by an award of council tax reduction	15-05-20 p, ph, f	Council tax rebate scam
25-03-20	Government announce intention to make home testing kits available	31-03-20 p, f, 17-04-20 p, f, 27-05-20 p, f	Phishing campaigns in England and Scotland direct victims to fake websites which claim to sell PPE equipment
17-04-20	Government announces job retention scheme	19-04-20 p, f	Fake job retention scheme phishing campaign.

Figure 8 cyber criminal response to current demand *m = malware, p = phishing, f = financial fraud* (Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple & Bellekens 2020).

According to European Union Agency for Cybersecurity (Enisa) phishing attacks spiked over 600% in the end of February 2020. This shows how good and convincing phishing can be when the time is right and people most vulnerable (Understanding and dealing with phishing 2020).

For a larger timescale we can see in Figure 9 that there is a huge increase after year 2017 in phishing sites comparing to malware sites. Phishing is used to carry malicious payloads more often and is proven to be effective. 96% phishing attacks happens via emails nowadays, only 3% through malicious webpage and 1% through phone calls (Must-Know phishing Statistics 2021).

Figure 9 Increase of phishing sites (Must-Know phishing Statistics 2021)

In the Figure 10 shows that China and USA were the most targeted countries by the end of March 2020. Because China and USA are one of the most populated countries in the world so when the pandemic stroke, those were also the first targets to strike.

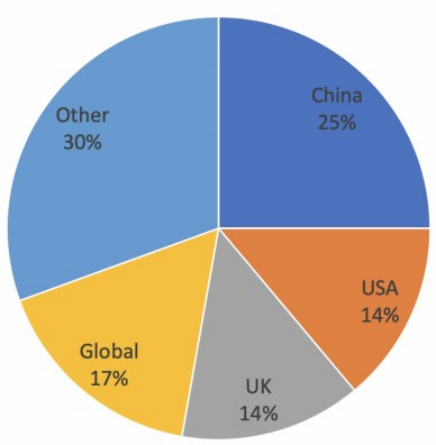

Figure 10 Cyber-attack across countries (Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple & Bellekens 2020).

7 Results

State-of-the-art result indicates that social engineering is still used highly amongst cyber criminals. It is seen in the studies as in real life that scams are everywhere. Also, when getting know to real life cases the attacks has been cleaver and attackers have known what to do and what to search for. As for the JYVSECTEC who this thesis is made for can benefit to the knowledge how big a problem the phishing has become just in 2 years and how big part social engineering plays of each attack. It is not something that should be overlooked but more like something to be teach further and deeper.

The main research question, how people are being exploited using social engineering methods is phishing. It has been popping up when searching the information and also in statistics. Phishing as in random phishing is where a large group of people is targeted with a scam. In that way when there is a large target group it is more likely to have also more victims who will fall in that scam. In this research phishing has been most used method and the nuances of it comes when figuring out the target group and the possible interest of that group. In this thesis there is examples of healthcare where fake doctor may offer some information that has not been published yet through email with malicious file or bank wants to verify account that might been hacked. These are something people should be aware of and always verify the source before downloading anything or giving personal information to anyone.

One of the sub-questions was how social engineering is used in 21st century and as stated in the main question it is more focused to the quantity than quality. Using phishing and emails to spread the malwares is more common and the threat has only risen because of covid-19 and the fear it has caused. Before the pandemic phishing was one of the used methods to implement malicious codes and to gain access to the private data but it was more difficult to lure people fall into the trap. It needed more social engineering skills and background checking and specific targets to reach the

goal. Pandemic offered easy way to scam people when searching information what is not easily available or even at all, after all the covid-19 pandemic was new to all of us.

Another sub-question focused the methods social engineering uses. Methods depends on what kind of attack is needed to gain the wanted result. The target can be specific when the more information is needed, and it is time consuming. But in those cases, the reward is usually higher. When the target is specified attack is usually against corporations or an organization such as healthcare. Targeting group of people has a bigger chance that someone is going to get hacked. When individual is the target, it usually means identity theft or some damage to the individual's life such as back account or other social account breach or even taking control victim´s computer to spread the virus further. In these cases, the prize is not as big as what getting from blackmailing corporation for their sensitive data. But not all methods of social engineering have to do with computers. Tailgating and eavesdropping can be an effective way to get the information needed or to get inside to a place where only restricted personnel is allowed. These methods doesn´t need necessary any IT equipment, unless used as a prop, just a cold nerve and social skills to influence people.

Last sub-question how to protect yourself of social engineering attacks can be tricky. Knowing the methods used and which methods are used more often it is possible to educate people and warn them about the attacks used at that time. Corporations are taking seriously phishing attempts and are giving training to personnel to minimize the chance of being attack. And in the time of pandemic the attacks are only increased. Often there is a warning in the bank's websites of ongoing phishing campaign in the name of the back and customers should never give credentials to anyone. Sadly, there is always someone that will fall into the attack and that just shows how good the attacks can be, anyone could be a victim before even realizing it. To protect yourself the main things to remember are to keep everything updated, never give credentials to anyone when asked and shouldn´t open any links or attachments, if the sender is unknow and you are not sure about it. The tricky part is that people

are often blinded by other politeness, kindness, and authorities. It is hard or even impossible to know if someone has hidden agenda when being polite. This is something every individual should think about without becoming cynical.

The information gathered for these results was mainly from the internet. Some good books were found from library where the topic focused more the methods used when scamming people. Security firms' webpages offered good knowledge of protection and the main idea how the attacks are conducted. These sources needed some filtering because firms are always advertising themselves so those should be ignored. Also comparing the information to others and finding same facts gave the insurance to the information. Some authorities such as WHO and TRAFICOM had statics that can be trusted and was used in this thesis not forgetting university research papers. Gathering information and trying to be truthful to the sources was the focus when choosing sources. Notable there is one source from our teacher who sadly left JAMK before starting this thesis. Nevertheless, I had his notes which I took from the lecture and even if it is not a good source, I wanted to add it in thesis. I could not find the same information from the internet as it was his own experience and knowledge about the subject. I would not doubt his knowledge because he was highly recognized teacher but could not get the confirmation to his source sadly.

8 Conclusions

I wanted to make a thesis about social engineering because it is more than just hacking. The human component is the most interesting part and how to adjust the attack depending on the target and the goal wanted. In the attacker's point of view the attack itself needs to be planned from the beginning. For example, if tailgating is needed, how to perform it and what kind of person attacker should be, to gain trust of people when confronting them face to face. In the victim´s point of view the situation is scarier, what and who can you really trust.

Before pandemic the situation was a bit different. Targets was mainly known such as different corporations, governments, different syndicates, and of course sometimes normal individuals. When covid-19 stroke, fear and lack of information gave great opportunity to hackers' attack to normal people, as they were easy prey. At least now we should realize the power of emotions and how it can be dangerous weapon when used right way. The fear has led to 600% increase of phishing attacks made after pandemic started. The email has been used to spread the false information and links or attachments to gain more information when opening them. Impersonating healthcare personnel it is easy to lure people because who would suspect them to be fraud in a time like this. But the time is perfect to social engineering attacks and to scam people when there is a chaos going on.

This led me thinking how to protect yourself or at least make you a less wanted victim. Updates and protections for devices, not just a computer are easiest ways to protect your property. There are more and more malwares on phones and tablets and that is why the applications should always be downloaded from the trustful source. This is easy part of protecting yourself which doesn't concern yet you're on consideration. When it comes to the attack itself then troubles start. Receiving an email or entering a webpage, how can you be sure that it is real? The doubt should be always there when browsing or reading an email. It can be exhausting and as seen there is a lot of people falling to these attacks without even noticing it.

Social engineering isn´t going anywhere as long as human factor exists. This is something that people should be aware of and if possible, more training and education concerning social engineering should be available. Now when computers are everyday life at home and in schools the attacks are not avoidable. We can only adapt and make sure that younger generation is well educated from the beginning to recognize all the threats that are behind the fun but useful internet.

The qualitative method I chose was a right for this thesis because the subject is abstractive. It would be hard to examine only through numbers because the human factor that exists. If the research was only about the data and statistics, then the quantitative method would be something to consider. But in this case when thesis was about human factor and how it relates to social engineering attacks, I feel the qualitative method was the only option.

For making this thesis was interesting even if it was a bit struggle to find a good angle to write it. I really wanted to find something different about social engineering attacks than phishing. But as it concluded phishing is the most used attack nowadays and it is included almost every attack made over internet. I find, for that reason thesis may be one-sided, but I tried to bring up the different kind of styles of social engineering like impersonation and eavesdropping that is something that might not come first in mind when talking about hacking. I wanted to make this thesis easy to read and to give a basic knowledge what to wait when hearing social engineering used when talking about cybersecurity. I found that there is a lot of information about social engineering but not all found in one cover. That is why I hope this thesis would gather the important points of social engineering attacks with some demonstration and real-life examples in it. I really hope I managed to achieve a goal to have easy approachable thesis with good basic knowledge as an introduction to social engineering through real-life cases.

I stumble to social engineering at school in class, and it was only a side note in a bigger attack we were hearing about. In my opinion, this thesis shows that social

engineering plays bigger part in cybersecurity and that said, it should be noticed more when talking about cyber-attacks, not only in workplace but schools also. The growing rate of attacks confirms that cyber criminals are not going away, on the contrary it feels that they are inventing more ways to pull successful attacks. That is why everyone should be alert and the education of cybersecurity in one form should start in early age when the first gadget with internet is in hand.

Refrences

2019 Phishing trends and intelligence report, The Growing Social Engineering Threat. N.d. PHISLABS report. Accessed on March 3, 2020. Retrieved from https://info.phishlabs.com/hubfs/2019%20PTI%20Report/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf

43 COVID-19 Cybersecurity Statistics. 2020. panda mediacenter. Accessed on November 23, 2020. Retrieved from https://www.pandasecurity.com/en/mediacenter/news/covid-cybersecurity-statistics/

73 Important Cybercrime Statistics: 2020/2021 Data Analysis & Projections. 2021. FinancesOnline webpage. Accessed on March 18, 2021. Retrieved from https://financesonline.com/cybercrime-statistics/

Abrams, L. 2020. Ransomware Gangs to Stop Attacking Health Orgs During Pandemic. Accessed on January 11. 2021. Retrieved from https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/

Barbosa, H. Breda, F & Morais, T. 2017. SOCIAL ENGINEERING AND CYBER SECURITY. Accessed on January 11, 2021. Retrieved from https://www.researchgate.net/publication/315351300_SOCIAL_ENGINEERING_AND_CYBER_SECURITY

Barry, C. 2020. Email threat types: Lateral phishing. Blog. Accessed on December 10, 2020. Retrieved from https://blog.barracuda.com/2020/08/21/email-threat-types-lateral-phishing/

CVE Common Vulnerabilities and Exposure. 2020a. CVE webpage. Accessed on March 25, 2020. Retrieved from https://cve.mitre.org/

CVE Common Vulnerabilities and Exposure. 2020b. CVE webpage. Accessed on March 25, 2020. Retrieved from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188

CVE. N.d. MITRE Corporation. Accessed on May 7, 2021. Retrieved from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9163

Dyre banking Trojan infections more than doubled. 2015. Help Net Security. Accessed on February 7, 2020. Retrieved from https://www.helpnetsecurity.com/2015/06/04/dyre-banking-trojan-infections-more-than-doubled/

Dyre. N.d. NJCCIC. Accessed on February 7, 2020. Retrieved from https://www.cyber.nj.gov/threat-profiles/trojan-variants/dyre

Ethical Principles for JAMK University of Applied Sciences Approved by the Student Affairs Board on 11 December 2018. 2018. jamk pdf-file. Accessed on May 3, 2021. Retrieved from https://www.jamk.fi/globalassets/opinto-opas-amk/opiskelu/pedagogiset-ja-eettiset-periaatteet/eettiset-periaatteet-11122018-en.pdf

Finnish institute for health and welfare. 2020. Coronavirus COVID-19. THL webpage. Accessed on March 28, 2020. Retrieved from https://thl.fi/en/web/infectious-diseases/what-s-new/coronavirus-covid-19-latest-updates/coronavirus-covid-19

Forbes.com Hacked In November, Possibly By Chinese Cyber Spies. 2015. Forbes webpage. Accessed on May 7, 2021. Retrieved from https://www.forbes.com/sites/thomasbrewster/2015/02/10/forbes-com-hacked-in-november-possibly-by-chinese-cyber-spies/

Hackers infect Forbes.com to spy on visitors: researchers. 2015. REUTERS. Accessed on May 7, 2021. Retrieved from https://www.reuters.com/article/us-forbes-cybersecurity/hackers-infect-forbes-com-to-spy-on-visitors-researchers-idINKBN0LE2F920150210

Hak5. N.d.a. USB Rubber Ducky. Hak5. Accessed on January 4, 2020. Retrieved from https://shop.hak5.org/products/usb-rubber-ducky-deluxe

Hak5. N.d.b. LAN Turtle. Hak5. Accessed on January 18, 2020. Retrieved from https://shop.hak5.org/products/lan-turtle

Hak5. N.d.c. WiFi Pineapple. Hak5. Accessed on January 18, 2020. Retrieved from https://shop.hak5.org/products/wifi-pineapple

Hakkarainen, P. 2020. Tunkeutumis- ja puolustusmenetelmät luento Jyväskylän ammattikorkeakoulussa

Hakkereilla on käsissään verta: kiristyshaittaohjelmalla tehtiin isku, potilas menehtyi ambulanssiin. 2020. Mikrobitin uutinen. Accessed on January 11, 2021. Retrieved from https://www.mikrobitti.fi/uutiset/hakkereilla-on-kasissaan-verta-kiristyshaittaohjelmalla-tehtiin-isku-potilas-menehtyi-ambulanssiin/f15b493f-d772-4589-b4e2-aa81131e9daa

Hyppönen, Mikko. @Mikko. (2020, March 18). *Public message to ransomware gangs: Stay the f away from medical organizations. If you target hospital computer systems during the pandemic, we will use all of our resources to hunt you down Twitter*. Accessed on January 11, 2021. Retrieved from https://twitter.com/mikko/status/1240225603565105152

Infosecurity. 2020. Keeping Your Backups Safe from Ransomware Attacks. Accessed on March 18, 2021. Retrieved from https://www.infosecurity-magazine.com/opinions/keeping-backups-ransomware/

JYVSECTEC by jamk. 2021. JYVSECTEC webpage. Accessed on May 3, 2021. Retrieved from https://jyvsectec.fi/about/overview/

Kiinassa todetut keuhkokuumetapaukset mahdollisesti koronaviruksen aiheuttamia. 2020. Terveyden ja hyvinvoinnin laitos. Accessed on November 23, 2020. Retrieved from https://thl.fi/fi/-/kiinassa-todetut-keuhkokuumetapaukset-mahdollisesti-koronaviruksen-aiheuttamia

Kitten, T. 2015. New Malware Attacks Prey on Banks. Accessed on February 7, 2020. Retrieved from https://www.bankinfosecurity.com/new-malware-attacks-prey-on-banks-a-8076

Labaree, R. V. N.d. Research Guides: Organizing Your Social Sciences Research Paper: Qualitative Methods. Research Guide. Accessed on February 6, 2020. Retrieved from https://libguides.usc.edu/writingguide/qualitative

Lallie, H., Shepherd, L., Nurse, J., Erola, A., Epiphaniou, G., Maple, C. & Bellekens, X. 2020. Cyber Security in the Age of Covid-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. Accessed on December 29, 2020. Retrieved from https://arxiv.org/pdf/2006.11929.pdf

Lateral Phishing. N.d. Barracuda. Accessed on December 10, 2020. Retrieved from https://www.barracuda.com/glossary/lateral-phishing

McAfee Labs. 2015. @McAfee_Labs. Twitter. Accessed on March 13, 2021. Retrieved from https://twitter.com/mcafee_labs/status/570765225873559552

Mitnick, K & Simon, W. 2002. The Art of Deception. Indianapolis: Wiley Publishing Inc

Must-Know phishing Statistics: Updated 2021. TESSIAN webpage. Accessed on May 7, 2021. Retrieved from https://www.tessian.com/blog/phishing-statistics-2020/

NATIONAL VULNERABILITY DATABASE. 2017. Nist webpage. Accessed on March 25, 2020. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2013-2729

Oberhaus, D. 2017. How a Wi-Fi Pineapple Can Steal Your Data (And How to Protect Yourself From It). Vice Webpage. Accessed on March 25, 2020. Retrieved from https://www.vice.com/en_us/article/pa39xv/pineapple-wifi-how-to-mitm-hack

Phishing awareness training that employees love. 2021. HOXHUNT webpage. Accessed on March 18, 2021. Retrieved from https://www.hoxhunt.com/gamified-phishing-training-platform/

Phishing Campaign Linked with “Dyre” Banking Malware. 2014. CISA. Accessed on February 7, 2020. Retrieved from https://www.us-cert.gov/ncas/alerts/TA14-300A

Phishing/Spear phishing. N.d. Enisa webpage. Accessed on January 18, 2020. Retrieved from https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing

Pneumonia of unknown cause -China. 2020. World Health Organization. Accessed on November 23, 2020. Retrieved from https://www.who.int/csr/don/05-january-2020-pneumonia-of-unkown-cause-china/en/

Q & A on COVID-19: Basic facts. 2020. European Centre for Disease Prevention and Control. Accessed on November 23, 2020. Retrieved from https://www.ecdc.europa.eu/en/covid-19/facts/questions-answers-basic-facts

Rolling updates on coronavirus disease (COVID-19). Updated 31 July 2020. World Health Organization. Accessed on November 23, 2020. Retrieved from https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen

ROP Chain. How to Defend from ROP Attacks (Basic Example). 2017. apriorit webpage. Accessed on May 7, 2021. Retrieved from https://www.apriorit.com/dev-blog/434-rop-exploit-protection

Ropek, L. 2020. Why the coronavirus pandemic presents a golden opportunity for hackers. SIW webpage. Accessed on Marcb 28, 2020. Retrieved from https://www.securityinfowatch.com/cybersecurity/news/21130847/why-the-coronavirus-pandemic-presents-a-golden-opportunity-for-hackers

Salahdine, F. & Kaabouch, N. 2019. Social Engineering Attacks: A Survey. Future Internet, 11(4), 89

Social Engineering: Impersonation. 2016. InfoSight. Accessed on January 18, 2020. Retrieved from https://infosightinc.com/blog/2016/01/29/social-engineering-impersonation/

Spear Phishing Attack. N.d. Mimecast webpage. Accessed on January 18, 2020. Retrieved from https://www.mimecast.com/content/spear-phishing-attack/

Spear Phishing: Real Life Examples. 2016. Infosec Resources. Accessed on February 7, 2020. Retrieved from https://resources.infosecinstitute.com/spear-phishing-real-life-examples/

Talamantes, J. N.d. What Is A Penetration Test And Why Do I Need It?. RedTeam webpage. Accessed on March 18, 2020. Retrieved from https://www.redteamsecure.com/blog/penetration-test-need/

The Social Engineering Framework. 2021. SECURITY THROUGH EDUCATION. Accessed on March 13, 2021. Retrieved from https://www.social-engineer.org/framework/attack-vectors/attack-cycle/

The Ultimate List Of Cyber Security Statistics For 2019. N.d. Purplesec webpage. Accessed on March 23, 2020. Retrieved from https://purplesec.us/resources/cyber-security-statistics/

TRAFICOM. 2019. TIETOTURVAN VUOSI 2019. Accessed on March 18, 2021. Retrieved from https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_tietoturvanvuosi_2019_WEB_sivuittain.pdf

TRAFICOM. 2020. Korona-aiheisia huijauksia on liikkeellä - mieti mitä klikkaat. Liikenne- ja viestintävirasto Kyberturvallisuus keskus webpage. Accessed on March 28, 2020. Retrieved from https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/korona-aiheisia-huijauksia-liikkeella-mieti-mita-klikkaat

Understanding and dealing with phishing during the COVID-19 pandemic. 2020. Enisa webpage. Accessed on March 18, 2021. Retrieved from https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic

US-CERT Warns Dyre Malware Used in Phishining Attacks. 2020. Phislabs webpage. Accessed on March 25, 2020. Retrieved from https://www.phishlabs.com/us-cert-warns-dyre-malware-used-in-phishing-attacks/

Using Regex to Find Sensitive Data on Your Network. N.d. ULTIMATE IT SECURITY.COM webpage. Accessed on May 7, 2021. Retrieved from https://www.ultimatewindowssecurity.com/webinars/register.aspx?id=260

Verkkourkinta. N.d. Yksityisyydensuoja webpage. Accessed on January 4, 2020. Retrieved from https://www.yksityisyydensuoja.fi/verkkourkinta

Whaling attack (whaling phishing). N.d. SearchSecurity. Accessed on December 26, 2019. Retrieved from https://searchsecurity.techtarget.com/definition/whaling

What is Forbes. 2021. Investopedia webpage. Accessed on May 7, 2021. Retrieved from https://www.investopedia.com/terms/f/forbes.asp

What is ngrok?. N.d. Ngrok website. Accessed on January 4, 2020. Retrieved from https://ngrok.com/product

What Is Phishing?. N.d. Cisco. Accessed on December 21, 2019. Retrieved from https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

What is social engineering? N.d. KnowBe4´s website. Accessed on March 18, 2020. Retrieved from https://www.knowbe4.com/what-is-social-engineering/

WHO julisti koronaviruksen kansainväliseksi kansanterveysuhaksi. 2020. Terveyden ja hyvinvoinnin laitos. Accessed on November 23, 2020. Retrieved from https://thl.fi/fi/-/who-julisti-koronaviruksen-kansainvaliseksi-kansanterveysuhaksi

Work at Ubiquiti! N.d. Ubiquiti webpage. Accessed on February 7, 2020. Retrieved from https://careers.ui.com

World Health Organization. 2020. Beware of criminals pretending to be WHO. WHO webpage. Accessed on March 28, 2020. Retrieved from https://www.who.int/about/communications/cyber-security

Appendices

Appendix 1. Phishing Demo with Socialfish

On the front page in Socialfish (Figure 11) one needs to select the social media which one wants to use for making the attack. After that the program asks the custom redirect URL (Uniform Resource Locator), which means the URL that the victim is redirected to after putting their credentials on the fake page. This is all that is needed. Socialfish will clone the social media page, in this case Instagram and give the URL that the victim needs to go to in order to get the attack to work (Figure 12).

Figure 11 Choosing the social media to use in attack

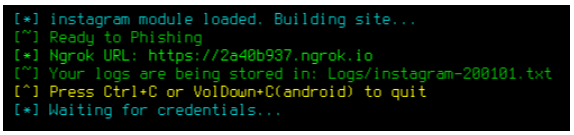

Figure 12 Ngrok give the URL to fake social media page

Socialfish is using Ngrok to make the tunnel for the traffic between a public address and Ngrok. It creates a public HTTPS URL for a web site, in this case Instagram. (What is ngrok? N.d). After this the Socialfish is waiting the victim to put credentials to steal.

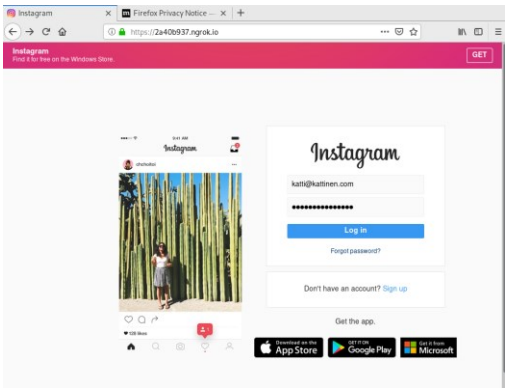

Figure 13 Fake Instagram page

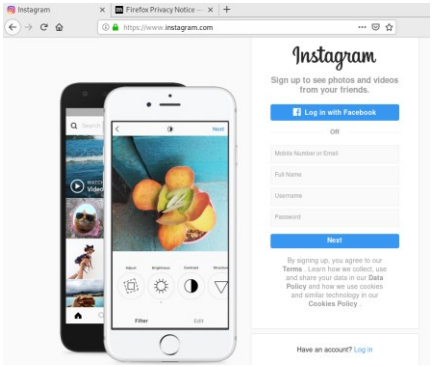

Figure 14 After the password has been put into the fake page, the redirection is made to go to the real Instagram

When the credentials are put to the fake Instagram page (Figure 13) and even if they are wrong Socialfish will show them to the attacker in plaintext (Figure 15). After the credentials are put into the fake page it is redirected to the real login page (Figure 14). This can make it slightly suspicious; however, in some case one just thinks one put the wrong credentials and continues like nothing happened.

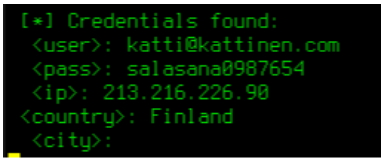

Figure 15 The credential stolen through fake page