Teemu Purhonen

PHISHING SUSCEPTIBILITY RATE FOR MULTINATIONAL ORGANIZATIONS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Purhonen, Teemu
Phishing susceptibility rate for multinational organizations
Jyväskylä: Jyväskylän yliopisto, 2023, 59 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Siponen, Mikko

Tässä tutkielmassa tarkastellaan tietojenkalasteluilmiötä ja erityisesti vertaillaan eri lähestymistapojen tehokkuutta tietojenkalasteluviesteissä. Tutkielman kohteena on verrata väärennetyllä verkkosivulla kirjautumistietoja pyytävien viestien tehokkuutta niihin, joissa uhria kehotetaan ainoastaan avaamaan linkki. Tutkielma tutkii myös englanninkielisten tietojenkalasteluviestien tehokkuutta, kun vastaanottajat eivät puhu englantia äidinkielenään.

Tietojenkalastelu määritellään teoksi, jossa uhria harhautetaan tiedon hankkimiseksi, mutta sen tarkemmat menetelmät ja tavat voivat vaihdella. Tietojenkalastelumenetelmiä ovat esimerkiksi smishing (SMS:n välityksellä) ja vishing (huijauspuhelu). Kohdennettu kalastelu kohdistuu tiettyyn yksilöön tai pieneen ryhmään, kun taas valastelu (eng. whaling) keskittyy korkea arvoisiin yksittäisiin kohteisiin. Tietojenkalasteluhyökkäykset voivat tähdätä tiedon keräämiseen tai haittaohjelmien injektoimiseen tietokonejärjestelmiin. Yleisiä taktiikoita ovat luotettavien tahojen teeskentely ja väärennettyjen kirjautumissivujen luominen. Tietojenkalasteluhyökkäyksiä vastaan tarvitaan vastatoimia, koska ne aiheuttavat 95 % onnistuneista kyberhyökkäyksistä. Hyökkäyksien torjuntaan tarvitaan kokonaisvaltainen lähestymistapa, johon sisältyvät tekniset tietoturvaratkaisut, tietoturvakäytännöt ja koulutus.

Osana koulutustaan erään monikansallisen organisaation kyberturvallisuusyksikkö on lähettänyt simuloituja tietojenkalasteluviestejä käyttäjilleen. Yksikkö on alkanut epäillä, että tietyt tietojenkalasteluviestityypit ja tietyillä kielillä lähetetyt viestit (englanti tai paikallinen kieli) ovat tehokkaampia kuin toiset. Tietääksemme tätä aihetta ole tutkittu aikaisemmin vastaavalla tavalla. Yksikössä haluttiin saada konkreettisia todisteita epäilyksille koulutuksen tehostamiseksi. Työntekijät saivat viisi simuloitua tietojenkalasteluviestiä, jotka oli lähetetty joko englanniksi tai heidän paikallisella kielellään, ja jotka edellyttivät joko pelkkää linkin avaamista tai lisäksi tunnistetietojen syöttämistä. Tämä tutkielman tulokset osoittavat, että pelkästään linkin avaamiseen perustuvat tietojenkalasteluhyökkäykset ovat menestyksekkäämpiä kuin tunnistetietojen syöttämistä vaativat hyökkäykset. Lisäksi tietojenkalastelusähköpostit vastaanottajan äidinkielellä ovat englanninkielisiä menestyksekkäämpiä. Tämä tukee aiempia tutkimuksia ja viittaa siihen, että paikallista kieltä käyttävät hyökkääjät saavuttavat suurempaa menestystä.

Asiasanat: koulutus, kyberturvallisuus, monikansallinen, simulaatio, tietojenkalastelu

ABSTRACT

Purhonen, Teemu
Phishing susceptibility rate for multinational organizations
Jyväskylä: University of Jyväskylä, 2023, 59 pp.
Cyber Security, Master's Thesis
Supervisor(s): Siponen, Mikko

This master's thesis focuses on phishing as phenomenon, and specifically comparing the effectiveness of phishing emails that ask for credentials on a fake login page versus (*Data entry* attack) those that just require the victim to click a link (*Click only* attack). It also explores the effectiveness of phishing emails written in English when the recipients are non-native English speakers (NNES).

Phishing is defined as a scalable act of deception to obtain information, but it may involve different methods and goals. Phishing methods such as smishing (via SMS) and vishing (fake phone calls). Spear phishing targets a specific individual or small group, while whaling focuses on high-value targets. Phishing attacks can aim to gather information or inject malware into computer systems, and common tactics include impersonating trusted entities and creating fake login pages. Countermeasures against phishing attacks are necessary, as they account for 95% of successful attacks. A comprehensive approach is required, including technical countermeasures, information security policies and anti-phishing training.

As part of their anti-phishing training, cybersecurity department of one multinational organization has sent simulated phishing emails to their users. They have started to suspect that certain types of phishing emails, and with certain language (English or local language), are more successful than others. They have wanted to get concrete evidence for their suspicion to be able to enhance their anti-phishing training. To our knowledge, there have not been previous studies for this topic in a similar setting. A simulated phishing study was conducted on employees of the company. The employees received five phishing emails in either English or their local language, and then either *Click only* or *Data entry* phishing attack. The anti-phishing training system tagged participants as susceptible if they clicked the link or provided their credentials.

This master's thesis reveals that *click only* phishing attacks are more successful than *data entry* attacks. Additionally, we found that phishing emails in participants' native or local language have a higher success rate compared to those in English, supporting previous findings and suggesting that attackers using the local language achieve greater success.

Keywords: anti-phishing training, cybersecurity, multinational, phishing, simulation

FIGURES

TABLES

TABLE OF CONTENTS

1 Introduction

This master's thesis focuses on explaining phishing as a phenomenon and how effective are phishing emails that ask the victim to submit their credentials on a bogus login page compared to those that just require the victim to click a link on an email. This master's thesis also studies how effective are phishing emails written in English when the recipient of the phishing email is a non-native English speaker (NNES). This analysis will be done utilizing an application that is developed specifically to send simulated phishing emails to multiple recipients and educate users about phishing. Four simulated phishing emails will be sent to an approximately thousand NNES employees during a period of nine months.

Lastdrager (2014) after completing his analysis of existing phishing research and literature, defines phishing as "a scalable act of deception whereby impersonation is used to obtain information from a target".

This definition of phishing is useful in providing an understanding of what phishing is, but it lacks information on the specific methods used to carry it out. The reason for this could be that there are multiple different methods to perform phishing and depending on which method to use, it could be called slightly different, however, the principles of phishing will remain the same, which is to acquire information from the victim that they may probably not want to (or should) give to the requester. This information is often sensitive like usernames and passwords. Probably when most people think about phishing, they will think about phishing *emails*, which seem to be the most used vector to deliver phishing messages. The word "email" was also mentioned in most phishing definitions that Lastdrager (2014) analyzed when he was looking for a consensual definition of phishing.

The definition from Lastdrager may not hold today, and it may require further analysis. In the definition, the goal of phishing is to acquire information, however, in media articles and some scientific research articles the goal of phishing has sometimes been something else than acquiring information. Phishing emails, or at least the same techniques, have been utilized by several advanced

persistent threat (APT) groups to distribute malware to target information systems (Chen et al., 2019) (Mascellino, 2022) (Gatlan, 2022). After injecting the malware, it is then up to the attacker what they want to achieve with it.

The malware could for example encrypt the target's files and data on the victim's computer system, and then demand ransom in exchange for the decryption key that can be used to try to recover the data. This kind of malware is called ransomware and the main motivation behind this malware is to ask for money, and not information, in exchange to recover the data. An example of this kind of malware is called WannaCry Ransomware which spread widely on a global level in 2017. (Mohurle & Patil, 2017)

1.1 Research motivation and need

The motivation for this study originated from a cyber security department of a private sector organization that have business operations in Nordic and Baltic countries. The department is responsible of educating the employees about phishing attacks and they have conducted anti-phishing training for their employees for multiple years. They have sent simulated phishing emails to the employees using a similar system like open source Gophish -tool that is developed specifically to send simulated phishing emails to multiple recipients. If the recipient of the phishing email is found susceptible to phishing by the system, they are given anti-phishing training.

Because the organization operates in countries where most of the population's native language is not English, they have sent these simulated phishing emails in both English and the predominant language of that country, i.e., the local language. They have noticed that the phishing emails written in the predominant language of that country, are perhaps more difficult for the employees to detect as phishing. However, they cannot be completely sure about this conclusion because the theme and the general content of the phishing emails that were written in English and phishing emails that were written in their native language have not been the same. So, the difficulty may not have come from the language that was used but from the general content of the phishing email itself.

To our knowledge, there have not been previous quantitative studies that focus on phishing susceptibility between English and a native language of a non-native English speaker (NNES) using simulated phishing emails in an organizational environment.

The type of simulated phishing attacks sent by the cyber security department has not all been the same. The system that is used to send simulated phishing attacks supports three kinds of attack types.

The first attack type is called a *click only*. In the *click only* -attack, the recipient of the simulated phishing attack gets an email that has a link to a website. If the recipient clicks the link, they are tagged as susceptible to phishing.

The second attack type is called a *data entry* which is quite similar to the *click only*. In the *data entry* -attack the recipient gets an email that has a link to a website. If the recipient clicks the link, they are directed to a login page, and if the recipient proceeds to log in, they are tagged as susceptible to phishing.

The third type of attack is called the *attachment*. As the name suggests, the recipient gets an email that has an attachment that they are asked to open. If the recipient opens the attachment, they are tagged as susceptible to phishing.

The cyber security department has noticed that the number of users who are susceptible to phishing varies between the different attack types, and it seems that when they conduct a *data entry* phishing attack, the number of recipients who are susceptible to phishing is much lower than in the *click only* phishing attacks. They want to get more reliable data for this rather than just relying on a hunch. The information can then help them enhance their anti-phishing training because they want to know where they should focus on their anti-phishing training.

1.2 Research questions

Based on the motivation and the needs of the organization's cyber security department, we derived three research questions.

1. Does language (English vs. local language) used in phishing emails influence the rate of falling into phishing attacks for non-native English speakers (NNES) in multi-national organizations (MNO)?
2. Which employees more easily fall for phishing by country?
3. Are *click only* phishing attacks more successful than *data entry* phishing attacks?

The *attachment* scenarios were left out of this study. The Difference between the *attachment* and the *click only* has been quite similar in the organization and having only two types of emails made the study simpler to execute and analyze.

1.3 Research ethics

Most of the employees of the organization were most likely aware that they will be trained with simulated phishing emails before this study started even though we didn't inform them in advance, however, they didn't know when they would get the phishing email and what was the content of the phishing email. The cyber security department of the organization has sent approximately four simulated phishing emails during a year for the past five years, and after each simulated phishing email scenario they have sent an informative email to all employees informing them about the simulated phishing email they have recently received. In this informative email, they were shown some statistics, training, etc. These past

simulated phishing emails and training are the reason why most employees should be aware they are targeted by this kind of training in the future as well.

Phishing emails are known to cause major financial harm and loss of sensitive information and intellectual property but also damage to reputation (Butavicius et al., 2016). In this study even if we are sending simulated phishing emails to train the employees, we want to keep the organization and its users anonymous. If the results of this study alongside the name of the organization and its employees would become public, it could cause reputational damage especially if the number of employees who succumbed to phishing is considered as high. Perhaps exceptionally good results could increase the reputation of the organization by showing the rest of the world how resilience they are against phishing attacks, however, the decision to keep the organization name secret was made early on before any data collection, and it was also the requirement from the management of the organization for this study.

Simulated phishing emails may also cause negative feelings, like anger, among participants and feelings of being betrayed (Goel et al., 2017). This further emphasizes the importance of employee anonymity. The point about simulated phishing emails should be to improve the cyber security posture on an organizational level rather than seeking and singling out employees who do not perform well in this kind of activity.

The report where we collected the user's behavior during the four simulated phishing was anonymized. The email addresses were removed, and the username was obfuscated. This report was then used to analyze the data to find answers to our research questions. Information that we collected was age group, gender, and which participants were susceptible to phishing and which were not.

In addition to causing negative feelings, simulated phishing emails could also cause stress among participants just like real phishing emails. In a study done by Jagatic et al., some of the participants performed mitigation methods to protect themselves, like changing their passwords or installing anti-malware software on their computers after being targeted by simulated phishing emails. (Jagatic et al., 2007).

Even if we didn't inform our participants about this study, and the simulated phishing emails in advance, we did try to limit participants stress and getting feeling of the need to perform mitigation methods against phishing, like changing their passwords, by informing them that this was a simulated phishing test in case they did succumb to phishing by immediately directing them to a webpage informing them that this was only a simulated phishing email sent by their organization.

Employees who did not succumb to phishing also had an opportunity to learn that the email was a simulated phishing test. Employees of the organization have been trained to report all suspicious emails to the cyber security department using an add-on that is installed on their email client. When reporting a simulated phishing email using this add-on, the employee will get an automated pop-up message from the email client thanking them for the report and their vigilance and informing them that this was a simulated phishing email.

If an employee reports an email that is not a simulated phishing email, they get a different automated pop-up message. This pop-up message confirms that the email is being reported to the cyber security department for further analysis. After few minutes, the employee will get a response back from the cyber security department that has their analysis of the email and what the employee should do next.

2 Literature review

2.1 Information systems and social engineering

Information systems consist of five components: (1) people, (2) activities, (3) technology, (4) data, and (5) network where all five components interact with each other. If any information system needs to be secured, we need to look at each component separately and make sure that correct countermeasures against threats targeting certain components are in place. The goal of the countermeasures is to ensure the systems' confidentiality, integrity, and availability, which are commonly referred to as the CIA triad. Confidentiality refers to that only legitimate users can access the data, integrity means that the data is not altered, and availability refers to that the data is accessible when it should be. (Raggad, 2010)

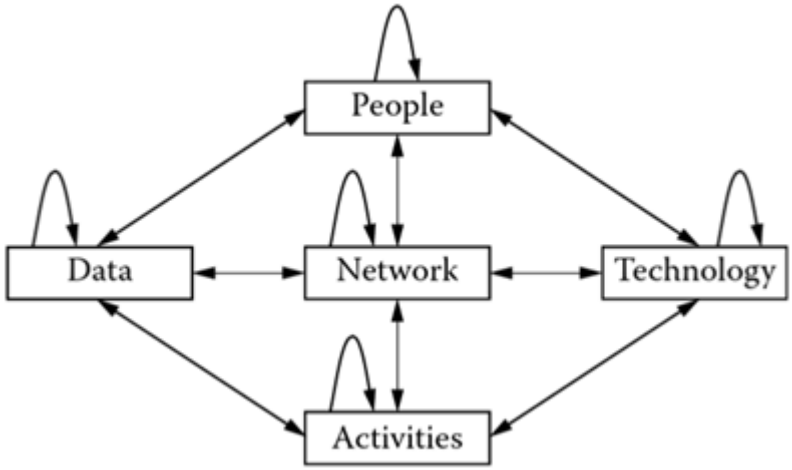

Figure 1: Computing environment with interactive components (Raggad, 2010)

Even back in the 1980s information systems were seen as competitive advantages to organizations and a way to lower expenses (Ives & Learmonth, 1984), however, today information systems could be considered more than a competitive advantage. One could argue that information systems are now vital to modern societies, individuals, and organizations.

Usage of social media, digital payment systems, and dependency on the internet has increased drastically in the past years. In March 2005, 5% of citizens in the United States answered on a survey that they use at least one social media site, and in February 2019 the percentage was 72% (Pew Research Center, 2021). Information systems are also important when we buy goods. E-commerce has started to take the room from the traditional "brick-and-mortar" shopping experience when the estimates say that by 2024, 21,8% of all sales are done using e-commerce when in 2015 it was only 7,4% (Keskin, 2022), and Sweden wants to become cashless on 2023 leading the world to a cashless society (Global

processing services, 2021). In Finland, The Digital and Population Data services is working together with the Finnish Police to develop a digital system that allows citizens to show proof of identity using a secure mobile phone application, and the project is planned to finish in 2023 (Digital And Population Data Services Agency). Organizations' dependency on the internet is also a big deal when in Finland, 43% of the organizations are incapacitated if they cannot access the internet for one day (Limnéll, 2020).

Cybercriminals are looking for the easiest and most efficient way to compromise or get access to the information systems by attacking against any of the five components which could then compromise the system's confidentiality, integrity, and/or availability. Attacks against information systems and their five components can take advantage of technical vulnerabilities, such as targeting protective systems like firewalls and antivirus tools. However, since information systems and these protective systems are used by people, attacks also focus on exploiting vulnerabilities that are human based. (Anderson, 2020) (Hunt, 2019)

Throughout history, it is often said by many people that human is the weakest link in any information system. Humans have many flaws or traits that cyber criminals can take advantage of and use to hack people. This hacking of people is often referred to as social engineering. Criminals using social engineering use psychology to manipulate the victim to achieve their goals (Aldawood & Skinner, 2019). These goals can be making people divulge confidential or sensitive information or installing malicious software on the computer system that can then give the social engineer or cybercriminal access to the system (Hunt, 2019). These social engineering attacks have also become very common among cybercriminals. According to a 2019 report by Proofpoint, less than 1% of cyber-attacks made use of technical vulnerabilities (Proofpoint, 2019).

It is not a surprise that attacks like these are common. Fixing human-based vulnerabilities is much harder than fixing computer-based vulnerabilities because every human is different from each other and even changing the behavior of one user can take a long time, certainly longer than fixing a vulnerability in a computer system. It would be convenient if security engineers could simply distribute a package of security patches to all their employees as they can do to most of their computers, servers, applications, and other information systems.

Social engineering has long roots in human history way before computers became a part of our everyday life. One famous example of social engineering is from Victor Lustig. Victor was born in 1890 and he was able to sell the Eiffel tower, not only once, but twice. He convinced top people in the French scrap metal industry that he was a French government official, and he told them that tearing down the Eiffel Tower has become mandatory due to engineering faults, costly repairs, and political problems. He then told them that the tower would be sold to the highest bidder. (Maysh, 2016)

Another famous social engineering attack is mentioned in Greek history around the year 12 000 B.C. when Greeks offered a giant horse to the Trojans as

a gesture of defeat but in reality, it was a clever way to get access inside the city walls, because the Greek soldiers were hiding inside the giant horse and when the Trojans moved the horse inside their city walls, they also gave access to Greek soldiers to the city. Eventually, this led Greece to victory (Hunt, 2019). This could only be a fictional tale instead of being an accurate piece of human history, however, it is a great description of social engineering attack where something malicious is disguised to look friendly. There is malware that is very similar with Trojan horse, which is called Trojan malware or Trojan virus. Trojan malware often uses the same or similar name as legitimate apps but if executed it can cause real harm for the information system (Microsoft, 2023).

2.2 Phishing

Phishing is a social engineering attack where cybercriminals try to obtain sensitive information from victims by taking advantage of human-based vulnerabilities using psychological manipulation (Alkhalil, Hewage, Nawaf, & Khan, 2021). This sensitive information can be passwords, usernames, and banking credentials. When they have collected the information, they can use them to conduct other attacks (Chen et al., 2019).

Phishing can also be used to trick the user to install malicious software on the victim's computer (Chen et al., 2019) (Mascellino, 2022) (Gatlan, 2022). One method used to achieve this is called macro virus (Särökaari, 2020). There are not many limitations to what this malware can do but it can be used to harvest sensitive data from the victim.

One of the most famous examples of phishing attacks happened back in 2016 during the United States presidential election. Hackers from Russia were able to hack into one of Hillary Clinton's accountant's computers and leak confidential emails to the public that arguably eventually led Hillary Clinton to lose the presidential election to Donald Trump. The email that was used in this phishing attack was simple but very efficient. It looked like a message from Google saying that someone has your password and that you should change it immediately. (Satter, 2017)

2.3 Different forms and types of phishing attacks

Phishing can be considered a computer-based social engineering attack which means that an electronic device is the attack vector. When the electronic device is the attack vector, the attacker doesn't have to be in physical contact with the victim (Hunt, 2019). This is one of the reasons why phishing and other compute-based social engineering attacks are so popular. When the attacker doesn't need a physical relationship with the victim, it reduces the likelihood of getting caught

and it makes the attack easier to do compared to human-based social engineering. Examples of human-based social engineering attacks are tailgating, shoulder surfing, and dumpster diving (Hunt, 2019).

Email remains to be the most used way of digital communication for organizations despite the increased usage of instant messaging systems like Microsoft Teams and Whatsapp. Phishing is, therefore, often done by email. According to a report from 2022, only 4% of phishing attacks didn't use email as the attack vector (Rosenthal, 2022). In 2017, half of all emails received by employees of Druk Green Power corporation, which is the largest electricity utility company in Bhutan, were either phishing emails or spam (Om, 2017).

One common tactic of phishing email attacks is to include a link to a malicious website created by the attackers in the email and try to trick the victim to click it to enter it (Jampen et al., 2022). The malicious website could impersonate bank or e-commerce site. Attackers can utilize botnets to a high extent to send phishing emails which allows sending emails to thousands of recipients at once and with minimum effort (Baruch, 2016).

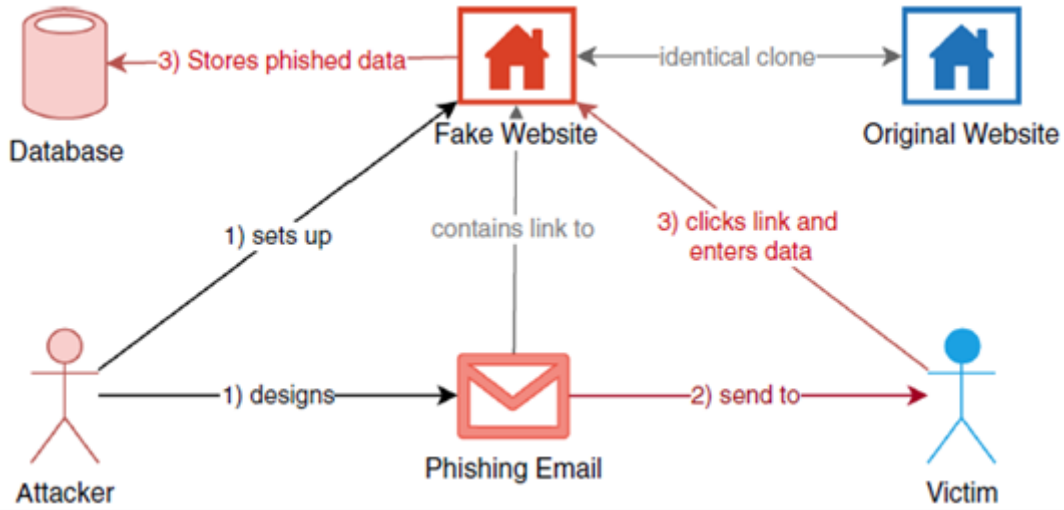

Figure 2: Example of an email-based phishing attack. (Jampen et al., 2022)

Botnet is a collection of computer systems that are remotely controlled by some entity, often a malicious one. These computer systems can, but are not limited to, personal computers, routers, and Internet-Of-Things devices like smart TVs. Computer systems are typically added to the botnet by infecting them with malware that then allows them to be added to the botnet. Figure 3 shows an illustration of a centralized botnet where the controller or the *Botmaster* enters a command to the command-and-control -server that then forwards the same command to the collection of computer systems that are part of the Botnet. (ENISA, 2011)

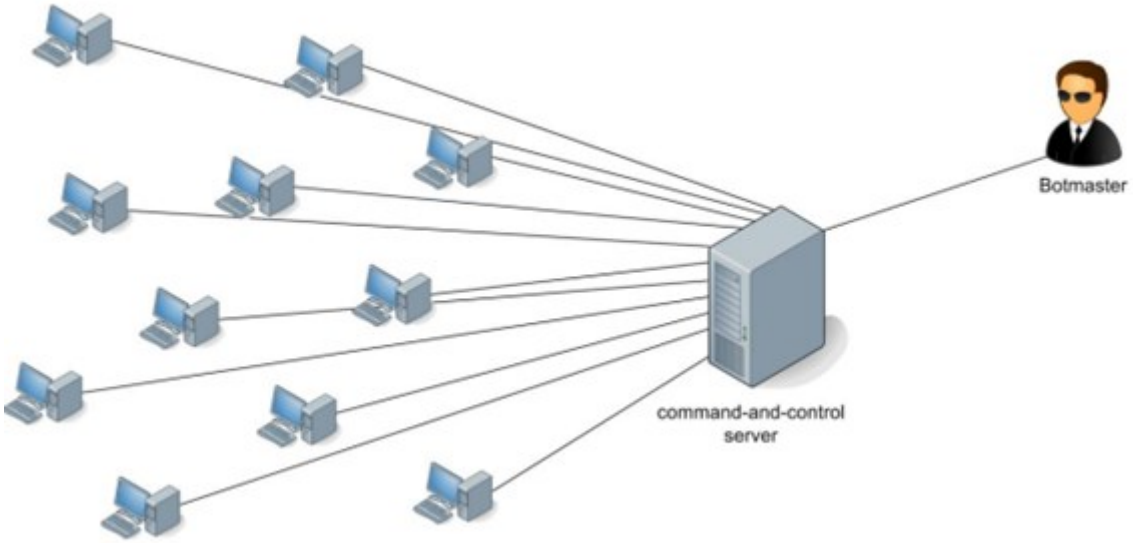

Figure 3: Illustration of Botnet (ENISA, 2011)

Email is the prevalent method to use in a phishing attack and botnets make it easy to use, however, it is not the only method to use in phishing. One other method to use in phishing is called smishing. In this attack the phishing message is sent to the victim's mobile phone using SMS messages (US Fed News Service, 2009).

Another form of phishing is called vishing. One quite well-known example of vishing is a fake technical support call where the social engineer impersonates a member of IT support team and makes claims that the victim's computer is infected with malware. They often ask the user to install a remote-control tool, that allows the attacker to remotely connect to the victim's computer. Once the *visher* has convinced the victim that their computer has a problem, they offer to "fix" the computer for a price. They could also try to harvest bank credentials or other valuable personal information. (Fruhlinger, 2020)

Phishing can also be categorized based on who the target is. When the social engineer targets a very small group of people or just one person, they can send more personal emails which can make the phishing emails very difficult to identify. This kind of phishing attack is called spear phishing. (Jagatic et al., 2007)

Spear phishers research their victims trying to acquire information about their interests, shopping preferences, banking information, hobbies, family, workplace etc. This information could be found on social media sites like LinkedIn and Facebook. From LinkedIn, they can potentially find the name of the organization where the target works and from the organization's website, they can potentially find the contact details of someone from the management. Combining information like this can get an accurate image of their target or targets. They can then use this built image of the victim they have to send highly personal and sophisticated custom-made phishing emails. They can for example impersonate the organization's CEO. Impersonating the CEO is quite a commonly used tactic and one form of Business Email Compromise (BEC) attack

(Federal Bureau of Investigation, 2021). The attacker could also impersonate their closest colleague, manager, or family member which would not be possible if the number of targets would be hundreds or thousands. Phishing emails impersonating someone from the organization's management team asking to click a link could make the target succumb to phishing even if they wouldn't normally do so. (Jagatic et al., 2007) (Hong, 2012)

Whaling is similar to spear phishing in that the number of targets is limited. The difference between whaling and spear phishing is that in spear phishing the target can be almost anyone, however, in whaling, the target is specifically a *high-value* target such as someone from the higher management of an organization like a CIO, CTO, or HR director, or even someone with great political power. An example of a whaling phishing attack is the previously mentioned phishing attack that took place in 2016 where the attackers targeted Hillary Clinton's accountant and got access to sensitive emails (Satter, 2017). (Warner, 2021) (Hong, 2012)

2.3.1 Information gathering vs injecting malware

The motive behind a phishing attack varies. The intention of some attacks could be to acquire information from the target whereas in some attacks the intention could be to inject malware. However, the same phishing and social manipulation tactics can be used in both types of attacks.

Phishing attacks that try to inject and install malware to the target computer system usually use have either, an attachment that is requested to open by the recipient, or a link that is asked to click. In some cases, if the victim simply opens the attachment, the damage is already done, as was the case in Follina zero-day vulnerability (Lakshman, 2022).

If the attachment is an office word file containing macro-virus, then the victim still has another chance to become alerted and prevent the malware from installing. Office macros can be disabled by default and office macro-virus requires that the macros are enabled. If the macros are disabled by default, and the user doesn't enable them when they open the file, the virus doesn't work. (Särökaari, 2020)

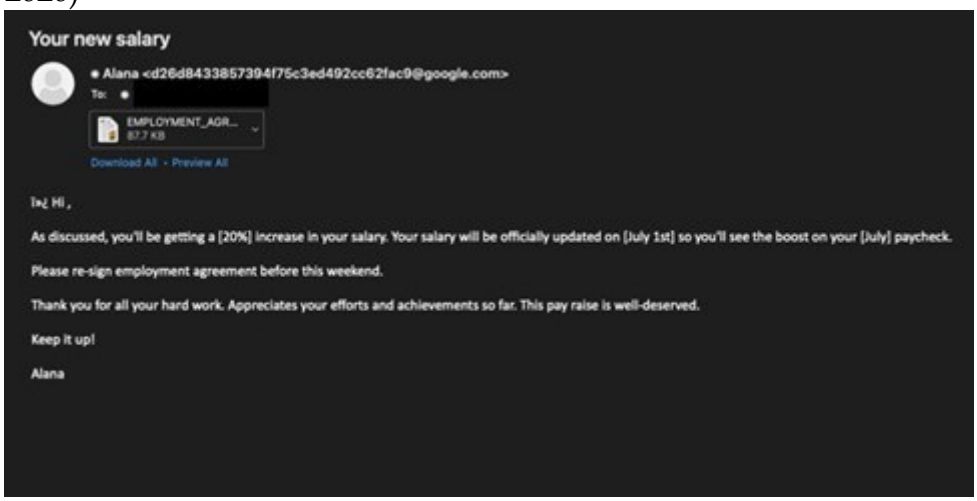

Figure 4: Phishing email delivering Follina (Lakshman, 2022)

Phishing emails with malicious links in them are trying to trick the user to click the link which could direct the user to a malicious website. If the motivation behind the attack is to inject malware into the computer system, simply entering the malicious website could be enough to get the computer system infected with malware. This kind of attack is called a drive-by download attack, and like the name suggests, you only need to *drive by* the website to get infected (Sood & Zeadally, 2016). Phishing emails with a link could also try to trick the victim to download the malware from the malicious webpage, by trying to convince them that the malware is some useful application or document.

Phishing attacks that want to gather information from the target try to convince the victim to share their sensitive and valuable information. One way to do this is to include a link to the email that directs the user to a fake login page that looks identical or at least very closely the same as any common famous login page, like Facebook, Gmail, or Netflix. They could try to convince the victim that their current password has expired or that someone else used or tried to use their account to log in, and they must act immediately to keep their account protected by changing their existing password by logging in first with their current username and password. However, once the user submits their current username and password, they will be sent to the social engineer instead. (Parrish et al., 2009) (Hoxhunt, 2019) This kind of phishing attack was used successfully against Hillary Clinton's assistant in 2016 (Satter, 2017) (Gilbert, 2016).

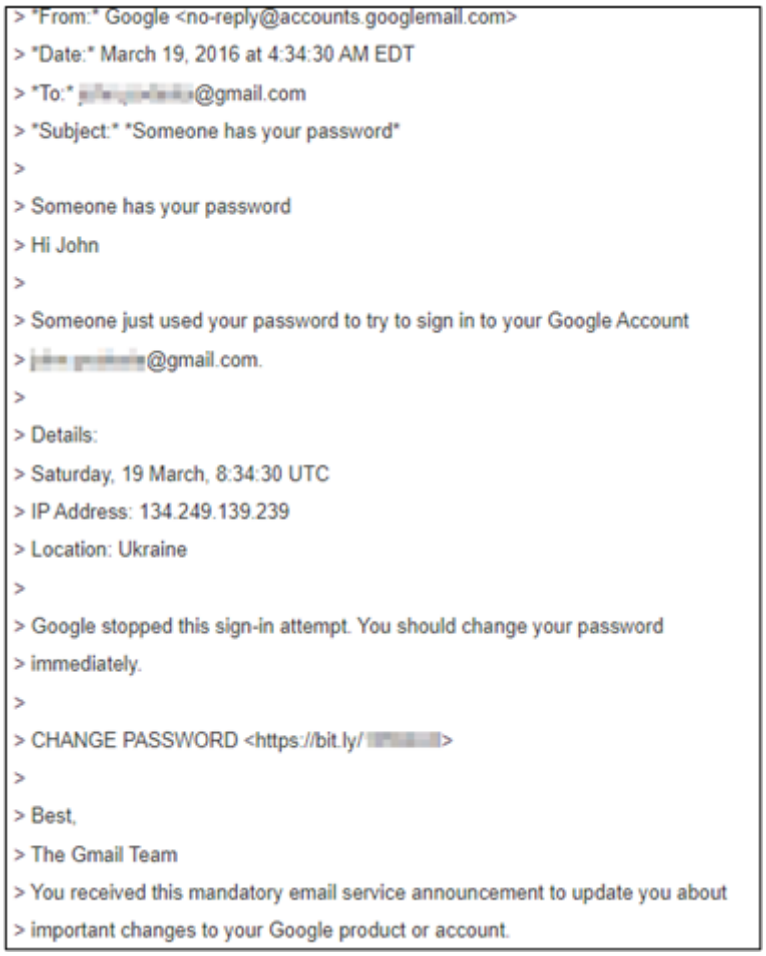
> "From:" Google <no-reply@accounts.googlemail.com>
> "Date:" March 19, 2016 at 4:34:30 AM EDT
> "To:" [redacted]@gmail.com
> "Subject:" "Someone has your password"
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [redacted]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/[redacted]>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.

Figure 5: Credential harvesting phish (Wikileaks) (Gilbert, 2016)

Another form of information-gathering phishing attack is the so-called Nigerian 419 scam or Nigerian Prince scam. In this phishing scam, the motivation is purely financial, whereas in previously mentioned attacks it could also be espionage (Grimmick, 2022). In this scam, the attacker tries to convince the target to share their bank account numbers. The attacker tells the victim they have just gotten a huge amount of money that they need to wire to a foreign account, and they ask their target if they are willing to accept this. Luckily this kind of attack or scam is not very sophisticated, and it is also quite old so many can identify it as phishing. (Ohaua, 2006)

2.4 Language used in Phishing emails - English vs native

Some may consider English being the *de-facto* -language on the Internet and IT world. When United-State is the biggest target of phishing emails (Simiou;Zand;Thomas;& Bursztein, 2020), and English is the most used language on the Internet (Web Technology Surveys, 2021) (Web Technology Surveys, 2023) (Internet World Stats, 2019), it doesn't come as a surprise that most phishing

emails are written in English (Simiou et al., 2020). English is so commonly used language in phishing emails, that companies providing phishing detection tools have been able to create AI algorithms that can detect some forms of phishing attacks, especially Business Email Compromise (BEC) attacks when the phishing emails are written in English (Gendre, 2021).

However, the dominance of the English language in phishing emails could be diminishing, or at least it is in some countries. Some security analysts have noticed an increased amount of BEC attacks, that instead of English, use Italian, Spanish, German, and Slovenian (Gendre, 2021).

In a five-month study during the Covid-19 pandemic about phishing and malware attacks, the researchers ranked top 10 countries receiving phishing email attacks. When we inspect the status of the top 10 countries where most of the population speaks English, over 90% of phishing emails were written in English. However, in France, Japan, and Brazil the usage of the English language is not dominant, instead, most of the phishing emails targeting recipients of those countries were written in their native language. (Simiou et al., 2020)

If cybercriminals start using the native language more often when they target non-native English speakers (NNES) as recipients, it could increase the succumbing rate to phishing among NNES' for a few reasons.

Technical countermeasures against phishing that rely on language detection and AI algorithms may not be that efficient against non-English phishing emails as the amount of data samples for English is drastically bigger than for any other language (Gendre, 2021).

Besides the challenges of some technical countermeasures, there are psychological reasons why NNESs are more susceptible to phishing when it's written in their native language. Research suggests at least two potential explanations for this.

Hasegawa et al. (2021) conducted a study on the challenges that non-native English speakers (NNES) face in identifying phishing emails. Their research involved participants from Germany, South Korea, and Japan. The study revealed that the participants received a greater number of phishing emails in English, and that they were more easily deceived by phishing emails written in their native language.

One possible explanation for becoming more easily deceived by phishing email written in their native language is that language barriers can negatively affect the building of trust between two parties, such as the social engineer and the potential victim (Tenzer et al., 2014). If the recipient of the phishing email does not trust the phishing email sender, the recipient is less likely to succumb to phishing (Moallem, 2019).

Another possible reason for this is that emails in English are simply ignored more often than emails written in the native language, and not much thought is given to the email whether it is an email from the legitimate sender or a phishing email. (Hasegawa et al., 2021)

2.5 Phishing success factors

One may wonder why phishing is even possible in the first place and why it is probably the most effective way to hack into any IT system. While the techniques and tricks employed by social engineers may not be novel, they are still successful. These tricks have been around for hundreds, if not thousands of years, dating back at least to the time of Greek mythology when the infamous Trojan horse tactic was utilized. (Hunt, 2019).

We have extended studies done by experts like Cialdini, Stajano, and Wilson where they have explained the principles that are used to conduct phishing attacks through human manipulation (Moallem, 2019). So why is phishing possible even though we know exactly what methods are being used against us? The answer to these questions is, that we humans are flawed, and we have errors that are not easy to correct.

Researchers in psychology have studied these human errors. In this chapter, we go through some of these flaws and errors that may explain why phishing attacks are possible from a purely non-technical perspective.

2.5.1 Human factor errors by Swain and Guttman

Authors Swain and Guttman in their book *Handbook of human reliability analysis with emphasis on nuclear power plant applications* (1983) explain five different human factor errors that might explain why social engineering and phishing attacks against people are successful. (Parsons et al., 2010)

1. Act of omission

The first error is called an act of omission which means that humans forget to perform some necessary actions (Parsons et al. 2010). Examples of this could be forgetting to delete a suspicious email after reporting it to authorities, not using secure payment solutions while doing online shopping, or forgetting to the install latest security patches on their devices.

2. Act of commission

The second error is called the act of commission. It means that people tend to perform incorrect actions, like deleting suspicious email but then not reporting it to the authorities (Parsons et al. 2010). Reporting the email to the authorities can allow them to block emails coming from the same sender.

3. Extraneous acts

The third error is called extraneous acts where the human does something unnecessary (Parsons et al. 2010). An example of an extraneous act is sharing sensitive information such as passwords or personal identification details over the phone or email to an unsolicited request when the act of sharing this information may not be necessary for the normal functioning of the task at hand.

4. Sequential acts

The fourth error is called sequential acts which means doing something in the wrong order (Parsons et al. 2010). An example of this can happen when the user gets a suspicious email and they intend to report and delete the email, however, instead of reporting the email first, they delete it. If the user doesn't know how to recover the email or if recovering the email is not possible, reporting the email is then not possible. Reporting the email to the IT department of the organization may allow them to block the sender and prevent future attacks.

5. Time errors

The fifth error is called time error which simply means that humans can fail to perform the task within the required time (Parsons et al. 2010). If the recipient of the phishing can report the email to the IT department as soon as they get them, the IT department can block the sender.

2.5.2 Cialdini's six principles of influence

Phishing is a type of cyber attack where the attacker tries to trick the victim into divulging sensitive information, such as usernames and passwords. To do this, attackers use tactics that are based on Cialdini's six principles of influence, which involve manipulating the victim. It's possible that attackers may not be aware that they are using these principles, however, they are still effective. It's worth noting that these principles are not only used in phishing attacks but also in other areas, such as business marketing, sales, and politics. (Moallem, 2019)

1. Reciprocity.

Reciprocity or obligation to repay is apparent in all human societies. This principle is used often in social engineering attacks. If the attacker can see that their victim is struggling with something, they can offer their help. When the attacker has helped the victim, they can ask for help in return. According to the reciprocity principle after getting help from someone, and then getting a request for help in return, most people want to return the favor. They feel that it is their obligation to repay somehow. (Moallem, 2019)

2. Commitment and consistency

Most of us have probably heard the inspirational quote: "Consistency is key to success". Sometimes the commitment or consistency of a user can indeed be the key for the social engineer to get access to confidential data or otherwise restricted areas. According to the commitment principle, many people will follow the same routines that they have learned and adapted, and they also follow the same way of thinking as before. Social engineers can take advantage of this. Moallem gives a great example of this. (Moallem, 2019)

In the example group of office employees have gone out for lunch. When they return, they need to unlock the door that is locked with a smart card. One of the employees holds the door for the others. A social engineer can take advantage of this and go into the area while one of the employees holds the door open out of courtesy. This technique is called tailgating. (Moallem, 2019)

3. Social proof

The social proof principle is the tendency for people to adopt the habits and ways of doing things that they see others doing, especially when they perceive those actions as correct or socially acceptable. The effect can be even stronger when multiple people engage in the same behavior. When a larger number of people perceive something as acceptable or the correct way of doing something, it tends to become more widely accepted as such. Also, when people are unsure about something they will start searching for what others think about it and then adopt the same way of thinking. (Moallem, 2019)

Unfortunately, this might have a serious negative impact. There can be a situation where a person with great power and good reputation has an incorrect or unsecured (from the perspective of cyber security) way of doing things. This way of doing could have been influenced by the social engineer or just bad luck. When others start following the same bad practice it opens the way for the social engineer. Popular social media influencers could also accidentally spread malicious website links to their followers.

4. Liking

"We like to say "yes" to people whom we like and know on a personal level." (Moallem, 2019) Social engineers, when trying to gather information from their victims, can try to acquire the status where they are liked by their victims. This can be done by trying to get a friendship –status by getting personal and asking personal questions, like how their family is doing, how was their day like or what are their hobbies. If the victim responds to these questions truthfully, the social engineer can claim that they also have the same hobby, or they did the same activities during the day. This is to acquire common interests which deepen the relationship between them and can make the social engineer more likable to the victim. (Moallem, 2019)

5. Respect for authority

Moallem (2019) says that "we obey those in charge". This is the key idea for understanding the respect of authority principle. It is said that out of all these principles, respect for authority is the most frequently used. It is often used in phishing and vishing. (Moallem, 2019)

Like in the example mentioned earlier in the vishing chapter where the social engineer claimed to be from IT support. IT support is also an entity that most users probably trust when it comes to IT-related questions. Also, in most companies, IT support can connect remotely to the user's computers. The victim has probably even experienced it first- or second-hand so the social if the social engineer requests to get a remote connection to the computer may not sound so out of the ordinary for the victim. Another example of using respect towards authority is Business email compromise (BEC) attacks where the social engineer impersonates someone from the organization such as CIO of the company (Federal Bureau of Investigation, 2021).

6. Scarcity

Moallem (2019) says that "Scarcity suggests that things are more valuable when they are less available." This is often being used in marketing. We see products with limited editions, that are a little different from the normal products, and we see products on sale, where the product is available with less money than before but with limited time. (Moallem, 2019)

There are no reasons why social engineers would not use this tactic. We already get legitimate advertisements from legitimate businesses that use the scarcity tactic, so it will make sense from a social engineering perspective to use those same messages but with malicious purposes. The email, or even text message, can be almost identical to the legitimate message, however, the big difference can be where the link directs or the content of the attachment. Instead of it directing or containing an offer or an advertisement it can be a virus or something else malicious. (Moallem, 2019)

2.6 Countermeasures against phishing attacks

Countermeasures against phishing attacks are not as simple as defending against pure technological attacks like malware and viruses. Countermeasures are much needed. According to Allan Parker, the research manager at SANS institute, 95% of successful attacks against organizations are due to spear phishing attacks (Weinberg, 2013).

Countermeasures against phishing include information security policies and anti-phishing training (Moallem, 2019). Technical countermeasures can also be effective, however, only to some extent, and relying mostly on them is not the most effective strategy (Wright & Marett, 2010).

2.6.1 Technical countermeasures

One main purpose of phishing is to acquire information from the target (Lastdrager, 2014), this information could be user credentials to some system or service (Särökaari, 2020) Multi-factor authentication (MFA) and two-factor authentication (2FA) can help victims who have gotten their credentials stolen. MFA and 2FA themselves cannot prevent theft, however, they can help prevent the attacker to use the stolen credentials.

Users who have enabled MFA or 2FA to the service, that supports it, are required to use another authentication method in addition to username and password (Arntz, 2017). The authentication method could be a time-based one-time code that is sent to the user by SMS (Rublon, 2022), or by a dedicated MFA mobile application like Microsoft Authenticator (Microsoft). If the user has MFA or 2FA enabled, and becomes a victim of credential theft, the attacker will also need access to their MFA or 2FA device or service. However, MFA and 2FA are not perfect and they come with their own challenges. Both are vulnerable to different kind of man-in-the-middle -attacks (MITM) (Funkhouser, 2022) and MFA fatigue attacks (Abrams, 2022), Also, these added security features create friction on the login -process to legitimate users (Doerfel, et al., 2019).

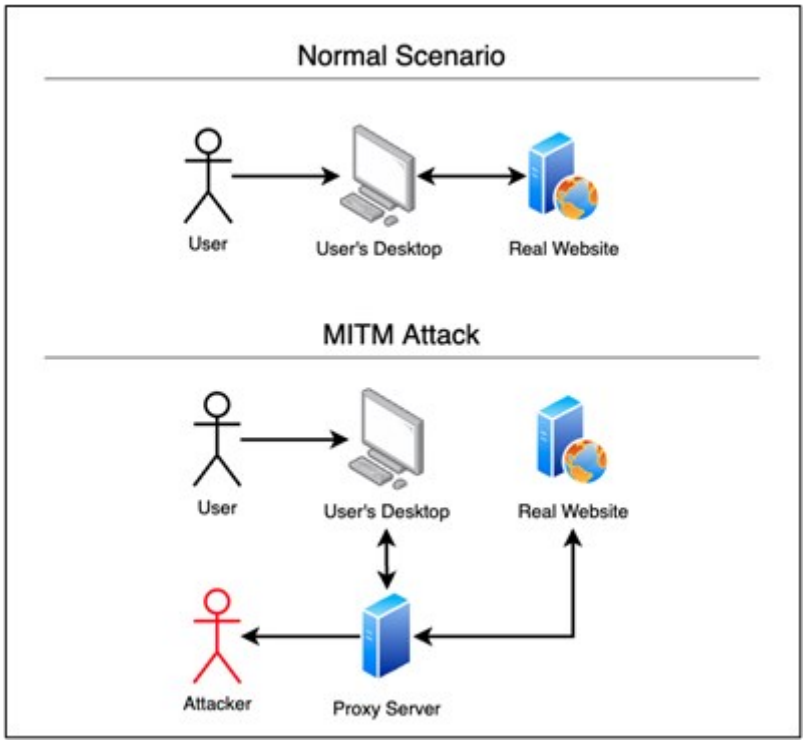

Figure 6: MITM attack (Funkhouser, 2022)

Like it was mentioned in chapter 2.3, phishing is often done by email so protecting the organization's email communications is important. Email security gateways are computer systems built to protect email traffic by directing all incoming and outcoming emails through the email security gateway. By directing

all incoming and outgoing emails through an email security gateway, the emails can be analyzed automatically or manually, and only legitimate emails can reach the intended recipient. Email security gateway can scan the emails, including the attachments, for any malicious files or links. Email security gateways can take advantage of various blacklists based on specific words on the email or the sender of the email (DuoCircle). This allows the email security gateway to block messages sent by malicious parties (Witts, 2022).

In addition to acquiring information from the target, phishing tactics are also used to distribute malware to the target system (Chen et al., 2019) (Mascellino, 2022) (Gatlan, 2022). Application whitelisting is another technical countermeasure against phishing. With application whitelisting system administrators keep a list of legitimate applications that are allowed to run on a system (Parmar, 2012). This measure can prevent the malware from executing, however, it doesn't prevent the malware executable to be stored on the machine. Some kind of alerting system should be put to place alongside the application whitelist that alerts a system administrator when a potentially malicious executable was blocked or downloaded so the system administrator can remove it from the system permanently.

Using a macro virus is one of the most common phishing attack methods (Särökaari, 2020). In this attack, the attacker infects a document with malicious macro (mostly in a Microsoft Office environment like Word) to install malware to the target system (Kaspersky). Disabling Office macros could be a solution to stop one of the most common attacks (Särökaari, 2020). However, Office macros do serve a legitimate purpose as well so, disabling them completely may interfere with the organization's business goals.

According to some estimates, technical countermeasures, including blacklists on the email security gateway level, can only block one-third of phishing campaigns (Wright & Marett, 2010). Some research suggests that secure email security gateways that use heuristic analysis can block up to 70% of phishing campaigns, however, a heuristic analysis could produce false positives which could even lead to lawsuits (Sheng, et al., 2009).

As important as technical countermeasures are, we need to look for additional solutions. We need to raise awareness of the threats and keep training people. Organizations should create information security policies that inform employees what acceptable behavior is and how the information system is protected, and what are employees' roles.

2.6.2 Information security policy

The objective of the information security policy should be to protect a specific system or asset. The policy should define certain protections to ensure the system's confidentiality, integrity, and availability. When confidentiality has been ensured we can be sure that only authorized personnel can access the system. Ensuring integrity, we can make sure that system does what it is supposed to, and that no one has made any unwanted changes to it. When availability has

been ensured we know that the system is available when it should be. (Goodman et al., 2008)

There are certain challenges and difficulties when it comes to information security policies that must be addressed. First, the policy cannot be against the organization's efficiency goals and practices (Niemimaa & Niemimaa, 2019).

Another challenge is to get the employees to understand the policy. The policy needs to be written in a non-technical way so everyone in the organization can understand it because threats can target the whole organization and any individual employee of the organization, not just those who work in IT or those that have good technical knowledge in general (Moallem, 2019). A great way to get users to understand the policy is to include them in the policy creation process. Employees tend to be more positive towards policies they had helped form. (Niemimaa & Niemimaa, 2019)

In addition to making the employees understand the policy, they need to comply with it. Compliance rating should be the main factor to measure the effectiveness of the policy. When people feel that they are in control of something, they tend to have a more positive attitude toward it (Moallem, 2019). If employees can feel that they are in control of the aspects of the information security policy, they should be more willing to comply with it. This again emphasizes the point that employees should be involved in the policy creation process

"Without active follow-ups, security policies go unread, educational programs fade away, and viruses come roaring back." (Thurman, 2003). Once the policy has been created and communicated to the employees, continuous work related to the issue is needed. Organizations cannot forget the policy and trust that landscape around the policy and asset remains the same forever. Technology changes rapidly and such things like Ransomware, IoT and other new technology give new opportunities and attack vectors to social engineers. Organizations are forced to revise their security policies. Even changes in employee behavior need to be considered. (Collett, 2017)

2.6.3 Anti-phishing training program

"Training is one of the main countermeasures against social engineering and phishing attacks…" (Parrish et al., 2009). The anti-phishing program has been recognized to significantly reduce employee's susceptibility to phishing emails, so all organizations should have one (Jampen et al. 2022).

The anti-phishing training program should be a part of the organization's global security awareness program. The purpose of the security awareness program is to raise awareness on various cybersecurity topics, social engineering included. Relevant and state of the art training helps employees to understand what might happen if they become a victim of phishing engineering attacks. Training material should also explain what the expected actions are if the employee becomes a victim of a cyberattack. (Parsons et al., 2010)

Organizations should identify their key individuals. Everyone in the organization can be a target of a social engineering or phishing attack, however, giving

extra training to key individuals can be beneficial since they might be getting targeted more than others (Moallem, 2019). Key individuals might have more access to different systems in the organization (e.g. IT system administrators) or by the nature of their work, they might be more susceptible to phishing attacks or are targeted more often (e.g. HR department and CIO). However, the training is also more than just teaching employees to react when something happens. The goal is also to teach employees to prevent future attacks by teaching them how to recognize these attacks and what is the correct approach when they see something suspicious that could be an attack (Parrish et al., 2009).

The anti-phishing program can include sending simulated phishing emails to employees. These simulated phishing emails are like phishing emails that real attackers use. However, if the employee clicks the link on the simulated phishing email or submits their credentials on simulated phishing web page, they are redirected to a website containing anti-phishing training. Employees should also be able to report phishing email attempts, both simulated phishing emails sent by their organization and real phishing emails sent by real attacks. Reporting methods and processes for both emails should be identical (Jampen et al., 2022).

The training material must be shown to the employee immediately after succumbing to phishing. The training material should explain clearly why this training was given to them, and how they could have recognized the phishing attempt. Employees who do not succumb to the phishing attempt but do not report the phishing email either could be given training explaining the importance of reporting the email and how to do it. If the employees can report a real phishing attack to the organization's cyber security department, they could be able to prevent more phishing emails from the same source from entering the organization by adjusting their technical countermeasures, which were explained in detail in chapter 2.5.1. (Jampen et al., 2022)

The anti-phishing program must be an ongoing process where the employees must be trained regularly because the accuracy to detect phishing emails degrades significantly over time. Studies have reported that the knowledge degrades after 6-8 months to the original value. (Reinheimer et al., 2020) (Kumaraguru, et al., 2009) (Renaud, et al., 2018)

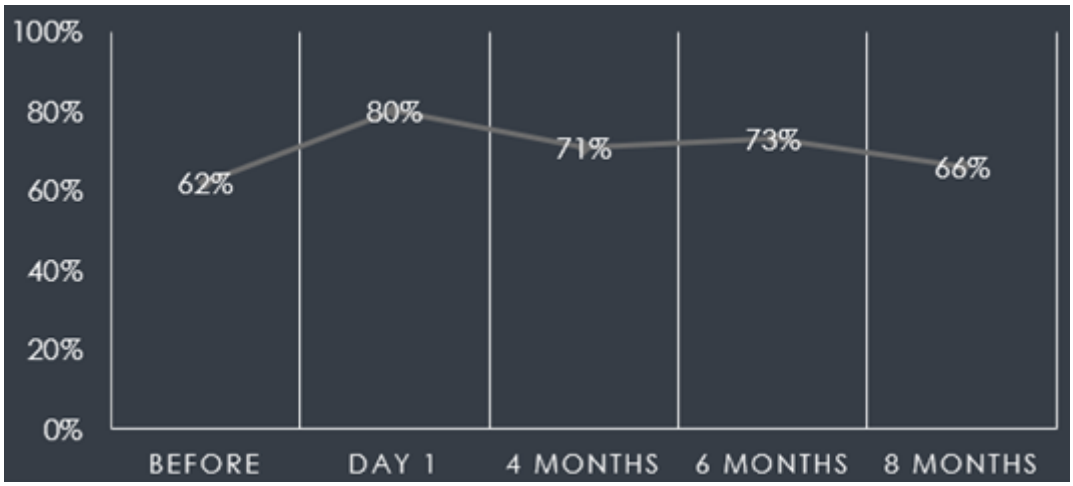

Figure 7: Accuracy to detect phishing emails before and after training (Reinheimer et al. 2020)

To enhance the effectiveness of the anti-phishing training program, it is recommended to establish an individual progression system. Employees who start to show improvement should be given more challenging simulated phishing emails and those employees who seem to fail to detect phishing emails constantly should be given easier phishing emails. This way those who want to learn more and seek challenges can be kept interested in the training, and those who face constant failures are given better chance to find success. However, this may be difficult to implement as there are no publicly available anti-phishing training tools that could support this important feature. (Jampen et al. 2022)

Besides teaching employees how to detect phishing emails, which could include inspecting URLs on an email, looking for the sender address, and learning differences between different file types, employees should also be taught about the underlying psychology of phishing email attacks (Jampen et al., 2022). One of the goals of anti-phishing training should therefore be changing employees' cognitive process so they suffer less from human factor errors, which are explained in chapter 2.5.2, and are less likely to become a victim of social influence/manipulation, like for those explained in chapter 2.5.3.

Simulated phishing emails may cause negative feelings, like anger, among participants and feelings of being betrayed (Goel et al., 2017). The goal for simulated phishing emails should be to improve the cyber security posture on an organizational level rather than seeking and singling out employees who do not perform well in this kind of activity.

Some employees could feel pressured about the training, and they could feel that they are being tested by their employers instead of being trained which could have a great impact on the employee's work-life balance (Jampen et al., 2022). It's therefore important that the reason and methods of the training are explained to all employees as well as any new employee entering the organization after the training program has initially launched.

Organizations should also remember that too much training, cyber security news, policy updates, etc. may cause employees to become overwhelmed by the situation and cause security-fatigue -effect (Jampen et al., 2022). Security fatigue could make employees feel hopeless about their cybersecurity, and even act recklessly (Stanton et al., 2016) which is the exact opposite of what the organization is trying to achieve.

3 Research methodology

This chapter presents the research methodology, the research questions, and problems. This research was done using quantitative methods.

3.1 Research problems and questions

The goal of this study is to find out how the content of the phishing email affects the phishing susceptibility rate. The phishing susceptibility rate is the number of participants who succumbed to phishing emails divided by the number of all participants.

We have two research questions on this study related to language effect.

- RQ1: Does language (English vs. local language) used in phishing emails influence the rate of falling into phishing attacks for non-native English speakers (NNES) in multi-national organizations (MNO)?
- RQ2: Which employees more easily fall for phishing by country?
    - Denmark vs. Estonia vs. Finland vs. Norway vs. Sweden

Past research suggests that people succumb to phishing emails written in their native language more often than to phishing emails written in English. Research suggests at least two potential explanations for this. The first explanation is that non-native English speakers tend to ignore all emails written in English (Hasegawa et al., 2021). Another explanation could be that language barriers may hinder the development of trust between two parties, such as the social engineer and the potential victim (Tenzer et al., 2014). Due to this lack of trust, the phishing email target may not believe or trust the sender of the phishing email, making the attack more likely to fail.

In the research done by Hasegawa et al. (2014) about phishing susceptibility for NNESs, there were some differences in phishing susceptibility rate between the three demographic groups. 25% of participants from Germany succumbed to phishing at least once when the phishing email was written in Germany and 14,1% succumbed to phishing when the phishing email was written in English. South Koreans and Japanese were better at avoiding phishing emails than their German counterparts.

The phishing susceptibility rate for South Koreans for phishing emails written in English was 14,5% and 6% for phishing emails written in their native language. The Phishing susceptibility rate for Japanese for phishing emails written in their native language was 10,1% and only 1,3% when the phishing email was written in English. Cultural differences between Europe and Asia could be significant and explain this difference. It will be interesting to find out if we can see any difference when all participants are located in Europe.

Our third research question is related to the phishing email type.

- RQ3: Are phishing attacks that only require the victim to click the link more successful than phishing attacks that requires the victim to submit their credentials?

In this context phishing susceptibility rate is the only success factor, i.e. phishing email with a 10% susceptibility rate is more successful than a phishing email with a 5% susceptibility rate.

The intention of a phishing email is not always the same. The intention could be to infect the target system with malware, or it could be to harvest credentials. We wanted to test which type of phishing attack our participants succumb to more. We suspect that phishing emails that harvest credentials are less successful than those just wanting to infect the target machine with a malware as harvesting credentials requires an additional step. Infecting the target machine with malware could only require the recipient to click a link on an email where harvesting the credentials requires the victim to submit their credentials on a fake login page. Even if the victim thought that the phishing email was legitimate, something on the login page could alert the victim and not submit their credentials.

3.2 Participants

We sent a phishing email to 10117 employees located in five different countries in Europe: Denmark, Estonia, Finland, Latvia, Lithuania, Norway, and Sweden. The participants are all employees of a company that has business operations in those countries. All office workers from these countries were targeted by our simulated phishing emails. The security team of this company has been sending simulated phishing emails to their employees in the past and it is part of their anti-phishing and cyber security training plan. Most likely many of the participants in this study were already somewhat familiar with this type of training.

The phishing emails sent to complete this study did not interfere with the company's training plan. The participants of this study would've gotten roughly the same amount of simulated phishing emails during the same period even if this study didn't have happened.

From the HR department, we got age group and gender information for 87% of the employees. 73% of the employees were men and 23% of the employees were women. The biggest age group was 45-54, and the second biggest age group was 35-44. 53% of the employees belonged to either of the previously mentioned age groups. 22% of the employees were younger than 35 years old and 23% of the employees were older than 55 years old.

We did not have any other information from the participants, such as their knowledge of information technology, their experience regarding phishing emails, or which department (e.g. HR, sales, customer service, or IT support) they

belonged to. Also, honoring the wishes of the company, the name or the field where this company operates is kept secret.

Participants were randomly divided into two groups. The other half would get all phishing emails in English whereas the other half would get them in their local language. Except participants in Lithuania and Latvia where all of them would get their phishing emails in English due to our limitations to translate English into Lithuanian and Latvian. Additionally, only 113 users in Lithuania and Latvia received all our phishing emails. Then the two groups were randomly divided into two other groups. Another half would get all their simulated phishing emails with click-only -type whereas the other half would get all their simulated phishing emails with data entry -type.

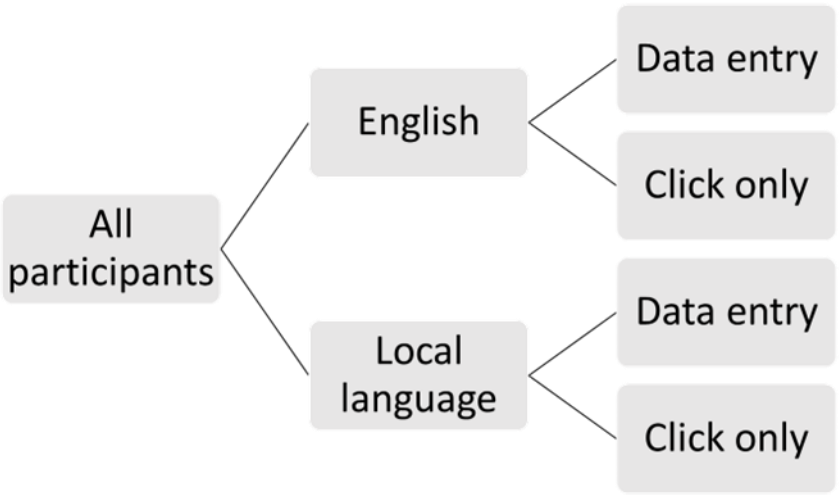

Figure 8: Distribution of participants

3.3 Simulated phishing emails

During the study, five simulated phishing emails were sent to over 10 000 participants from a system like open-source Gophish that is designed to be used to send simulated phishing emails to multiple participants. However, not all participants received our phishing emails due to their email clients rejected the email for some reason. This could happen because either they had left the company, or their email box was full. 8 642 participants received all five phishing emails. All the simulated phishing emails are based on real phishing emails that were able to bypass some email security gateway.

There were two types of phishing email attacks: (1) *click-only* -phishing attacks and (2) *data entry* – phishing attacks. The general content of the email on both attack types was the same and each email had a link that the participant was asked to click. Difference between *click only* and *data entry* emails was what happened after the participant clicked the link.

If the participant clicked the link on a *click only* -email, they were forwarded to a web page that told them that this was a simulated phishing attack organized by their organization. When the participant clicked the link, they were tagged as *susceptible to phishing* by the system.

If the participant clicked the link on a *data entry* -email, they were forwarded to a login page that asked for their email address and password. The login page was made to look like it belonged to Microsoft. If the participant proceeded to give their email address and password, they were forwarded to a web page that told them that this was a simulated phishing attack organized by the organization. After the participant had clicked the link and submitted their credentials, they were tagged *as susceptible to phishing* by the system.

The system also collected the email address they used to log in but not the password. Displaying the email address helps to indicate if the participant thought that the email was legitimate. E.g. if the user used their real email address like firstname.lastname@organization.com they probably thought that the email was legitimate, however, if they used *a burner* email address like asdasd@asfd.com they were probably somewhat suspicious about the legitimacy of the email and/or the login page.

All five emails had different themes so the participants would not learn from the theme alone that the email was a phishing attempt. The first email was a notification about unpaid invoices. The second email was a notification that someone had sent files to the recipient using OneDrive and Dropbox like file-sharing services. The third email was a notification about an expired password. The fourth email was a notification from a printer. The fifth email was a notification from HR about changes in employee health policy.

All phishing emails were translated from English to Danish, Estonian, Finnish, Norwegian, and Swedish by experts in that language. Phishing emails written in English were also proofread by a language professional. Phishing emails were not translated to Latvian or Lithuanian as we didn't have any one to proof read them, hence all Latvian and Lithuanian users received all five phishing emails in English.

3.3.1 Phishing email 1: You have unpaid invoices

The first phishing email simulated an invoice phishing email, that has been seen in the wild multiple times with different variations (Xero, 2022). The email is sent from a fictional member of the financing team in a fictional bank. We wanted to impersonate a real bank to make the email look more legitimate, however, we didn't have contacts with any of the banks that operate in all countries that were in the scope of this study. We didn't want to impersonate any real bank without their consent therefore we ended up using a fictional bank instead.

In this phishing email we tried to convince the recipients to click the link by taking advantage of Cialdini's fifth principle of influence; respect of authority, by claiming to be from a bank and the finance team. We also planted a false sense of

urgency, which is a common tactic used in phishing attacks, in the email by claiming that they have multiple unpaid invoices where the due date is on Monday, Tuesday or Friday. The email was sent on Monday morning so the first invoice would expire in one day.

There is one very clear indicator of phishing that could alert anyone who would receive this email, and therefore not click the link. That is the name of the bank. Because we used a fictional bank that has no real customers, the recipient of this message should get alerted and suspect that this was indeed a phishing attempt. The email also doesn't have any additional details about the invoices, like the amount of money to be paid or to whom.

There are several good practices that can help prevent falling victim to a phishing attempt like this. One is to never use the link used in the email. If an email makes a claim of unpaid invoices or employs other deceptive tactics to encourage the recipient to click on a link or open attachments, it is recommended that the recipient logs in to their bank account using a legitimate login page that they are familiar with (such as through saved bookmarks or a trusted mobile app), verify the status of their account, or contact the bank's support team.

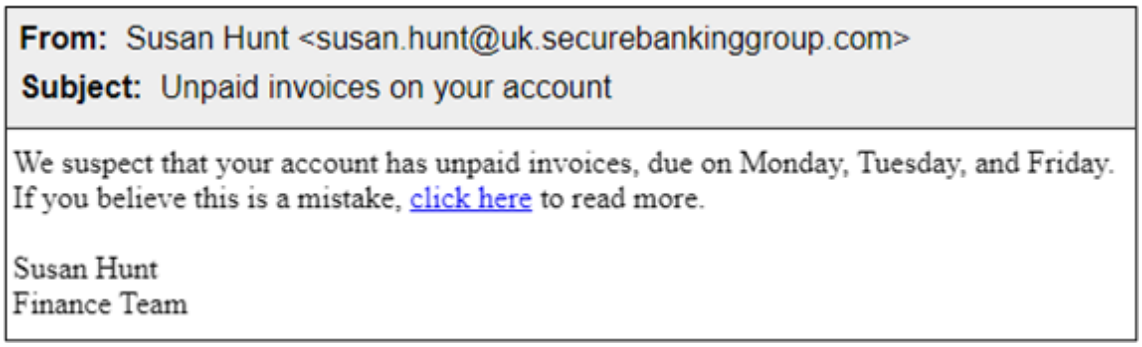

Figure 9: Phishing email 1: Unpaid invoices

3.3.2 Phishing email 2: Someone shared files with you

The second phishing email simulated a file-sharing phishing email, which is similar to phishing emails that have been seen in the wild that claim to be sharing a file or files from Dropbox or WeTransfer. (Meskauskas, 2022) (MailGuard, 2021)

This phishing email has the same indicator of phishing that the first phishing email had. No file-sharing service called *Securefileshares.com* exists. This should alert anyone who would receive this email, and therefore not click the link.

One could argue that not everyone can know all possible file-sharing services that anyone can use, and that's probably true. However, in a situation when an email from an unknown source is received, it could be a good idea to pause for a few seconds and think if they were expecting an email like this, and they could also look up the name of the service or company used in the email from online to find out if it's real or if it's associated to any phishing attacks.

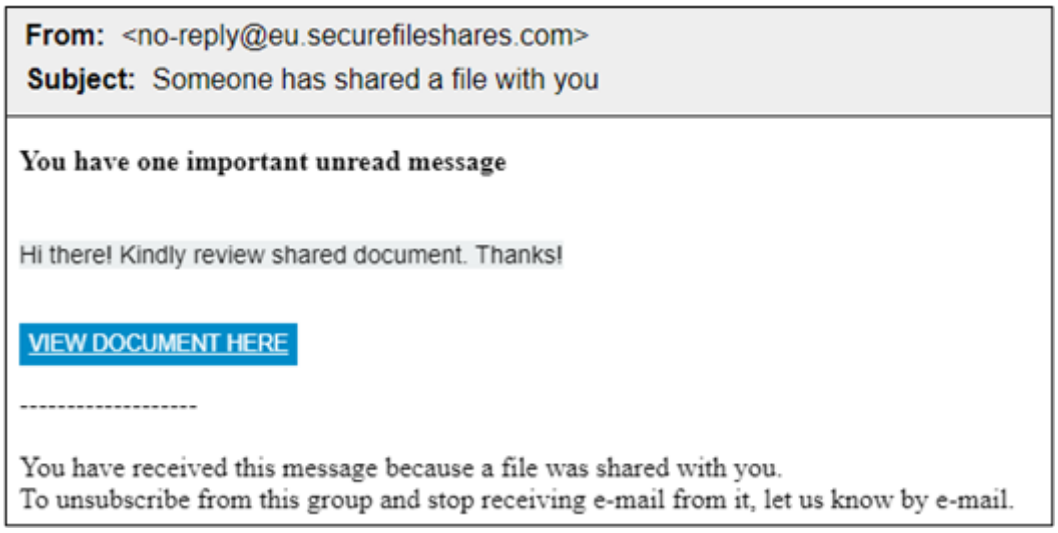

Figure 10: Phishing email 2: File share

3.3.3 Phishing email 3: Expired password

The third phishing email simulated an expired password phishing attack where the idea is to trick the victim to believe that they must update their password to continue working or using the service, and attacks like this have also been seen in the wild, and they are quite effective (Brecht, 2020).

This attack relied on respecting the authority -principle as the sender claimed to be from the IT support by sending the email from the *IT Support* using email address *admin@itsecuritymessage.com*. We also planted a false sense of urgency claiming that the recipient will only have two days to update their password and urged them to do this immediately.

The organization doesn't inform their users about expired passwords like this so, just the content of the email alone should be an indicator that there is something wrong with this email and that it could be a phishing attempt. The second indicator is the sender's email address. If it would be the organization sending this email, they would use their domain address as their sender address, like *it-support@organization_name.com*. The third indicator is the link address. If the recipient would hover over the link, they could see that the URL has nothing to do with their organization which you can see in figure 12.

Figure 11: Phishing email 3: Expired password

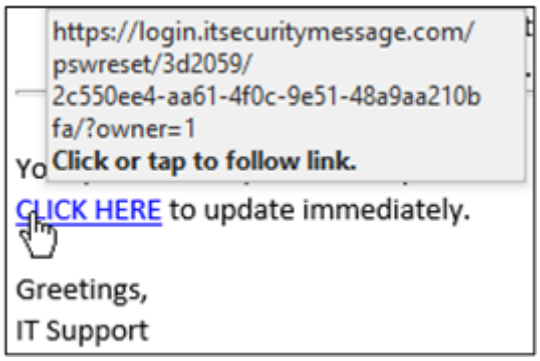

Figure 12: Phishing email 3: Expired password -link

3.3.4 Phishing email 4: Notification from printer

On the fourth phishing email, we simulated phishing attacks that take advantage of a feature that is available on most multifunctional printers (MFP). It is possible to scan a document on MFP and then send that document via email to the selected recipient(s). In the wild phishing attacks like these have been seen impersonating Xerox MFP, and if the recipient clicks the link they are then asked to sign in, which would result in cybercriminals receiving their credential information (Online Threat Alerts, 2018).

Major indication of phishing in this case is the sender, and more specifically, combination of *friendly name* and *sender address*. The friendly name being *Konica* and the sender address being *new@eu.printerhelpdeskp.net*. When inspecting them further one could see that they are not related which could alert the recipient and not succumb to this phishing attempt.

Another way the recipient could notice the phishing attempt is to pause for a few seconds and think for what the reason could be they got this email. MFPs don't typically send emails by themselves. The user usually has to do it themselves. So, unless the user just happened to send a real document from MFP they should be alerted because they wouldn't be expecting this kind of email. Another possible indication of phishing is how the email wants the recipient to access the

document. In this organization, most of the MFPs send the document attached to the email instead of using a link.

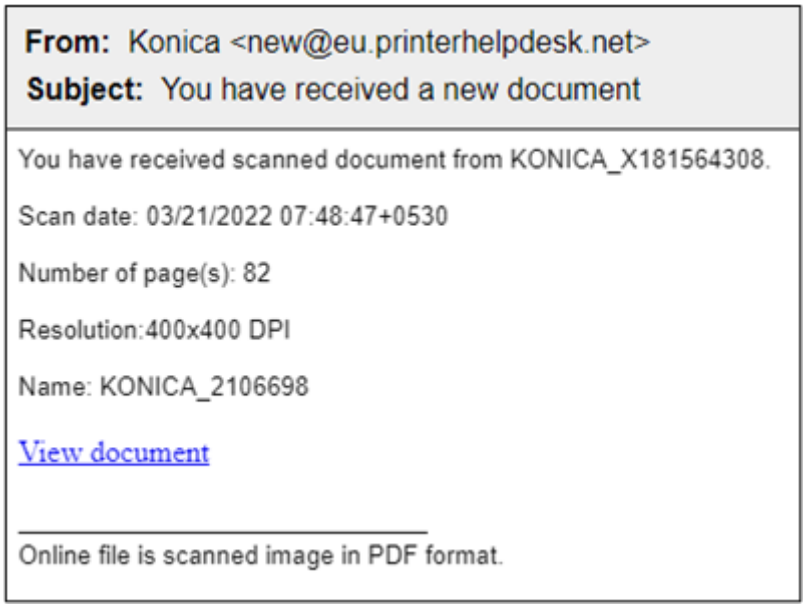

Figure 13: Phishing email 4: Printer notification

3.3.5 Phishing email 5: Changes in employee health policy

This study was done during the global Covid-19 pandemic and during this time security analysts suspected increase in phishing emails impersonating the HR department. On the fifth and final phishing email, we decided to impersonate the HR department and take advantage of the global Covid-19 pandemic. We sent a Covid-19-related phishing email in which we informed the users about a new employee health policy that all employees are required to adhere to. We included a link that they were asked to click to accept this new policy, which of course wasn't real.

Similar clues were present in this phishing email as in *phishing email 3: Expired password*. If it would be the HR department of the organization sending this email, they would use their domain address as their sender address, something like *HR-no-reply@organization_name.com*.

We suspect that this phishing email could be more difficult to identify as phishing than the *phishing email 3: Expired password*, where we also impersonated the internal department of the organization. The tone of the email is much more restrained. There are no ultimatums or strict deadlines in this email. The employees of this organization may have also received emails from the HR department before about a wide variety of topics whereas emails from IT support asking to change the password should never happen.

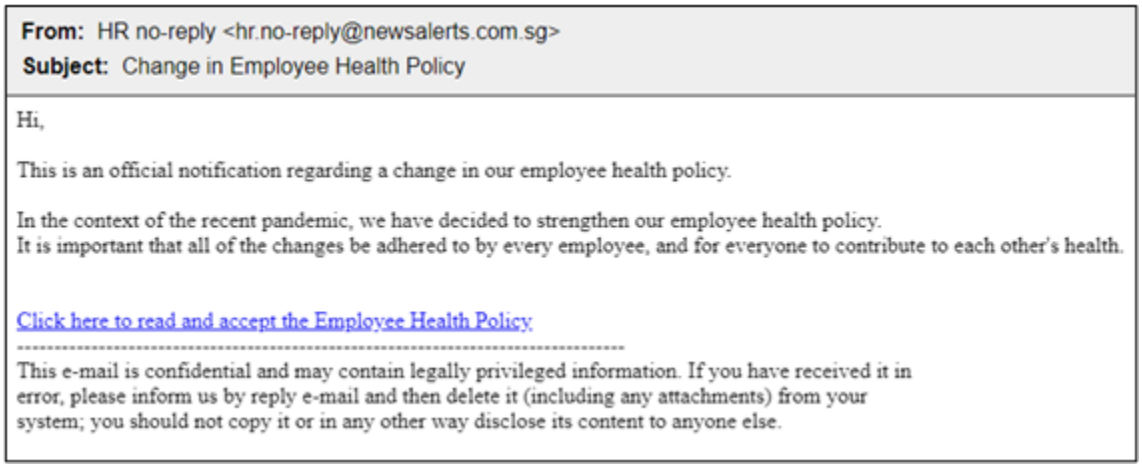

Figure 14: Phishing email 5: Message from HR

4 Results

In this chapter, we go over the analysis of the results and we try to find the answers to this master's thesis research questions.

- RQ1: Does language (English vs. local language) used in phishing emails influence the rate of falling into phishing attacks for non-native English speakers (NNES) in multi-national organizations (MNO)?
- RQ2: Which employees more easily fall for phishing by country?
    - Denmark vs. Estonia vs. Finland vs. Norway vs. Sweden
- RQ3: Are phishing attacks that only require the victim to click the link more successful than phishing attacks that require the victim to submit their credentials?

Lastly, we look at the success rate for the five phishing emails and investigate if we can see if there were any differences between them.

Latvia and Lithuania user were deliberately left out from deeper analysis because they received phishing emails in English, however, users in said countries are still part of the English (*combined*) results.

4.1 RQ1: Does language (English vs. local language) used in phishing emails influence the rate of falling into phishing attacks for non-native English speakers (NNES) in multi-national organizations (MNO)?

The result shows there's a significant difference between the local language group and the English group (Waldχ^2 = -14.330, p <.001) in phishing email avoidance performance from the first phishing email to the fifth phishing email (see Table 1.). The phishing rate in the Local language group is significantly higher than in the English language group. This is consistent in all five phishing emails (see Table 2.).

The analysis was conducted on IBM SPSS 28.0. Multivariable logistic regression, with the use of a generalized estimating equation (GEE) approach (Schober & Vetter, 2018) was used to compute odds ratios (ORs) with 95% CIs for the odds that a phishing email would be clicked during a campaign. Specifically, GEE was used to examine the statistical significance of the effects of the language used in phishing emails on succumbing behavior.

Table 1: Results of Generalized Estimating Equations (GEE) Multiple Regression Analysis for language type

Parameter	**B**	**Std. Error**	**95% Confidence Interval**			**Hypothesis Test**	
			Lower	Upper	Wald Chi-Square	*df*	*Sig.*
(Intercept)	-3.615	.1221	-3.854	-3.375	-29.595	1	0.000
En/Local-Local	-1.022	.0713	-1.162	-.882	-14.330	1	0.000
En/Local-English	0.000	.	.	.	.	.	.

When we inspect the results by country and by language group (see Table 2), we can see that in all countries and language groups, the English group was significantly better at avoiding phishing attempts than the Local language group. The biggest difference between the English language group and the Local language group was in Norway where the English language group was 30% units better at avoiding phishing attempts. In Estonia, the difference between the English language group and the Local language group was the least significant, when in the English language group, the victimization rate was only 10% units lower than in the Local language group.

When looking at the combined results of all countries we can see that the English language group was 24% units better at avoiding phishing attempts than the Local language group. The difference between the English and Local group in Denmark is almost the same as the combined results for all countries with 25% units. Finland and Norway are not that far behind with a 20% units' difference between the English and Local language groups.

Table 2: Victim number and victimization rate (categorized by *country* and *language group*)

Country	Denmark		Norway		Finland		Estonia		Sweden		Combined	
	(n=1355)		(n=2909)		(n=804)		(n=307)		(n=3154)		(n=8642)	
Language	Local	English	Local	English	Local	English	Local	English	Local	English	Local	English
Phishing email 1	25	5	127	13	1	1	3	1	100	7	256	27
Phishing email 2	19	4	48	24	4	4	3	1	37	16	111	51
Phishing email 3	89	58	232	220	58	24	18	14	144	122	541	451
Phishing email 4	43	22	58	50	28	24	6	3	72	41	207	144
Phishing email 5	100	20	314	58	90	6	9	4	223	82	736	174
N of victims	276	109	779	365	181	59	39	23	576	268	1851	847
N of participants	680	675	1458	1451	403	401	153	154	1577	1577	4271	4371
(%)	**0.41**	**0.16**	**0.53**	**0.25**	**0.45**	**0.15**	**0.25**	**0.15**	**0.37**	**0.17**	**0.43**	**0.19**

Note: *Victimization rate (%) = the number of victims / the number of emails successfully delivered*

We kept track of each participant's performance when it comes to avoiding phishing attacks. We were able to find out that some participants succumbed to phishing at least twice during our study, some participants even succumbed to phishing all five times (see Table 3.). We called participants who succumbed to phishing twice or more *repeated victims*.

These results confirm what we saw in victim number and victimization rate (see table 2.) phishing emails in the local language are more successful than phishing emails in English when the target is NNES. 8% of all the participants who received the phishing emails in their local language succumbed to phishing at least twice, while only 2% of all the participants who got the phishing emails in English succumbed to phishing at least twice.

Table 3: N of repeated victims (categorized by *country* and *language group*)

Repeated victims	Denmark		Norway		Finland		Estonia		Sweden		Combined	
	(n=1355)		(n=2909)		(n=804)		(n=307)		(n=3154)		(n=8642)	
Language	Local	English	Local	English	Local	English	Local	English	Local	English	Local	English
Get phished 2x	42	10	118	42	26	6	8	2	88	24	282	84
Get phished 3x	5	2	15	2	8	0	0	0	15	2	43	6
Get phished 4x	7	0	11	3	0	0	0	0	5	1	23	4
Get phished 5x	0	0	1	0	0	0	0	0	2	0	3	0
Total N of repeated victims	**54**	**12**	**145**	**47**	**34**	**6**	**8**	**2**	**110**	**27**	**351**	**94**
N of participants	680	675	1458	1451	403	401	153	154	1577	1577	4271	4371
(%)	**0.08**	**0.02**	**0.10**	**0.03**	**0.08**	**0.01**	**0.05**	**0.01**	**0.07**	**0.02**	**0.08**	**0.02**

4.2 RQ2: Which employees more easily fall for phishing by country?

In the context of chapter 4.1 we established that across all countries the English language group is better at avoiding phishing emails compared to the Local language group. To obtain the answer to RQ2, our attention can be directed solely towards the victimization rate within each country.

We were able determine that Participants in Norway were significantly the least successful at avoiding phishing emails with an overall victimization rate of 39%. The results indicate that participants in Norway demonstrated he lowest levels of success in evading phishing attempts across all five phishing emails, except on the fourth phishing email. Participants in Finland were the least successful at avoiding the fourth phishing email. 6,5% of the participants in Finland succumbed to that phishing attempt whereas only 3,7% of the participants in Norway succumbed the same phishing attempt.

The results show that participants in Estonia were the most successful at avoiding phishing emails with a total victimization rate of 20% (*Victimization rate (%) = the number of victims/ the number of emails successfully delivered)*. However, it must be noted that this success was not uniform across all phishing attempts. Specifically, the Estonian participants achieved the highest levels of success only on two phishing attempts: in the fourth and the fifth.

Overall, the second most successful country to avoid phishing emails was Finland with a victimization rate of 30% followed quite closely by Sweden with a victimization rate of 27%, and Denmark with a victimization rate of 28%.

Table 4: Victim number and victimization rate (categorized by *country*)

Country	Denmark		Norway		Finland		Estonia		Sweden		Combined	
	(n=1355)		(n=2909)		(n=804)		(n=307)		(n=3154)		(n=8642)	
	n	%	n	%	n	%	n	%	n	%	n	%
Phishing email 1	30	2,2 %	140	4,8 %	2	0,2 %	3	1,0 %	107	3,4 %	282	3,3 %
Phishing email 2	23	1,7 %	72	2,5 %	8	1,0 %	4	1,3 %	53	1,7 %	160	1,9 %
Phishing email 3	147	10,8 %	452	15,5 %	82	10,2 %	32	10,4 %	266	8,4 %	979	11,5 %
Phishing email 4	65	4,8 %	108	3,7 %	52	6,5 %	9	2,9 %	113	3,6 %	347	4,1 %
Phishing email 5	120	8,9 %	372	12,8 %	96	11,9 %	13	4,2 %	305	9,7 %	906	10,6 %
Total	**385**	**28,4 %**	**1144**	**39,3 %**	**240**	**29,9 %**	**61**	**19,9 %**	**844**	**26,8 %**	**2674**	**31,4 %**

Note: *Victimization rate (%) = the number of clicks/ the number of emails successfully delivered*

When we inspected the number of *repeated victims* by country (see table 5.) we can see the same results as in victim number and victimization rate by country, although the differences between countries are not that significant. The least number of *repeated victims* was in Estonia (3% of the participants) and most were in Norway (7% of the participants).

Table 5: N of repeated victims (categorized by *country*)

Repeated victims	Denmark (n=1355)	Norway (n=2909)	Finland (n=804)	Estonia (n=307)	Sweden (n=3154)	Combined (n=8642)
Get phished 2x	52	160	32	10	112	366
Get phished 3x	7	17	8	0	17	49
Get phished 4x	7	14	0	0	6	27
Get phished 5x	0	1	0	0	2	3
Total N of repeated victims	66	192	40	10	137	445
(%)	**0.05**	**0.07**	**0.05**	**0.03**	**0.04**	**0.05**

4.3 RQ3: Are phishing attacks that only require the victim to click the link more successful than phishing attacks that require the victim to submit their credentials?

The result shows that there's a statistical significance between phishing attacks that only require the victim to click the link (click only) and the phishing attacks that require the victim to submit their credentials (data entry) (Waldc2 = 469.890, p <.001) on succumbing behavior from first to last phishing email (see Table 6.). The succumbing behavior caused by the *click only* (CO) type of phishing email is significantly higher than the *data entry* (DATA) type of phishing email.

The multivariable logistic regression analysis was conducted on IBM SPSS 28.0. With the use of a generalized estimating equation (GEE) approach (Schober & Vetter, 2018) was used to compute odds ratios (ORs) with 95% CIs for the odds that a phishing email would be clicked during a campaign. Specifically, GEE was used to examine the statistical significance of the effects of the type of phishing emails (IV) on succumbing behavior (DV).

Table 6: Results of Generalized Estimating Equations (GEE) Multiple Regression Analysis for phishing email type

Parameter	**B**	**Std. Error**	**95% Wald Confidence Interval**		**Hypothesis Test**		
			Lower	*Upper*	*Wald Chi-Square*	*df*	*Sig.*
(Intercept)	-1.715	0.0383	-1.79	-1.639	2000.375	1	0.000
[Email type=1]	-1.103	0.0509	-1.202	-1.003	469.89	1	0.000
[Email type=2]	0.000	.	.	.	.	.	.

Note: Email type = 1 (click only), Email type = 2 (Data entry)

Looking at the combined results for all countries the difference between CO and DATA is consistent in all five phishing emails (see Table 7.). The overall victimization rate for CO phishing emails is 29% units higher than in DATA phishing emails.

Upon closer examination of the results by a country, we discovered some differences when compared to the *combined* results. Specifically, two cases were identified in which CO and DATA phishing emails demonstrated equal levels of success. On the first phishing email, an equal number of participants in Finland succumbed to phishing when only one participant from each group succumbed to phishing. On the second phishing email, an equal number of participants in Estonia succumbed to phishing emails when only two participants from each group succumbed to phishing.

When further investigating the results for phishing email type success rate by a country we can see that the success rate difference between CO and DATA phishing emails for Estonia is noticeably the lowest out of all countries when CO phishing emails were only 23% units more successful than DATA phishing emails. The highest difference regarding the success rate was in Denmark where CO phishing emails were 34% units more successful than DATA phishing emails.

Table 7: Victim number and victimization rate (categorized by *phishing type*)

Country	Denmark		Norway		Finland		Estonia		Sweden		Combined	
	(n=1355)		(n=2909)		(n=804)		(n=307)		(n=3154)		(n=8642)	
Phishing type	CO	DATA	CO	DATA	CO	DATA	CO	DATA	CO	DATA	CO	DATA
Phishing email 1	29	1	115	25	1	1	3	0	86	15	235	42
Phishing email 2	19	4	57	14	6	2	2	2	42	9	128	31
Phishing email 3	115	32	301	149	58	24	24	8	166	93	673	310
Phishing email 4	62	3	93	14	47	5	9	0	97	15	311	38
Phishing email 5	84	36	231	140	72	24	11	2	225	78	625	282
N of victims	309	76	797	342	184	56	49	12	616	210	1972	703
N of participants	693	662	1468	1441	400	404	157	150	1581	1575	4354	4288
(%)	**0.45**	**0.11**	**0.54**	**0.24**	**0.46**	**0.14**	**0.31**	**0.08**	**0.39**	**0.13**	**0.45**	**0.16**

Note: click only (CO), data entry (DATA).

4.4 Overview of the five phishing email and their success rate

It's important to note that even though this company has some employees working with finance tasks such as paying invoices, this company doesn't work in finance sector. This is relevant to note when analyzing results of the phishing email 1.

Some of the five phishing emails were more successful than others (see table 8.). We suspected that this would be the case and noticed it during the study. The phishing email that impersonated the organization's IT department that claimed that the recipient's password is about to be expired was the most successful out of the five. 11,3% of the participants succumbed to that simulated phishing email. The second most successful phishing email impersonated the organization's HR department, and its victimization rate was 10,5 %.

However, it's interesting to see that these two emails were almost equally successful among our participants even though the nature of the emails is quite different. The e*xpired password* email is very blunt and direct and tries to plant a false sense of urgency whereas in the *Changes in employee health policy,* the tone of the language is much more restrained and there are no ultimatums or strict deadlines on this email.

The other three phishing emails (1, 2 & 4) were noticeably less successful. Probably the most notable disparity between these emails and the previously mentioned ones is the sender. Phishing emails 3 & 5 claimed to be from some department of the organization (IT support and HR) whereas Phishing email 1

was from a fictional bank, Phishing email 2 was from an unknown sender via file sharing service, and Phishing email 4 was from a printer.

Table 8: Victim number and victimization rate (categorized by *phishing email*)

	Phishing email 1	Phishing email 2	Phishing email 3	Phishing email 4	Phishing email 5
Subject	You have unpaid invoices	Someone shared files with you	Expired password	Notification from printer	Changes in employee health policy
N of victims	283	162	992	351	910
Victimization rate	3,2 %	1,8 %	11,3 %	4,0 %	10,5 %

5 Discussion and conclusion

The main points and findings of this study are explained in this chapter as well as the weaknesses and limitations, practical implications, and future research ideas.

5.1 Main points and findings of the study

This master's thesis objective was to explain phishing as a phenomenon. Another objective was to find out how effective are phishing emails that ask the victim to submit their credentials on a bogus login page compared to those that just require the victim to click a link on an email, and how effective are phishing emails written in English when the recipient of the phishing email is non-native English speaker (NNES). We also studied which participants by country were most susceptible to phishing.

Phishing is a social engineering attack where cybercriminals try to obtain sensitive information, usually by email, from victims by taking advantage of human-based vulnerabilities using psychological manipulation (Alkhalil, et al., 2021). This sensitive information can be passwords, usernames, and banking credentials. Lastdrager (2014) defines phishing as "a scalable act of deception whereby impersonation is used to obtain information from a target". However, phishing techniques can also be used to trick the victim to install malicious software onto their computer (Chen et al., 2019) (Mascellino, 2022) (Gatlan, 2022).

Phishing attacks can be called by different names based on how it is done technically. *Smishing* refers to SMS-based attacks (US Fed News Service, 2010) and *vishing* for voice call-based attacks (Fruhlinger, 2020). Phishing can also be called by different names based on how many targets it has or who the target is. *Spear phishing* attacks target only a few selected victims (Jagatic et al., 2007), and *whaling* targets high-value targets like CEOs (Hong, 2012). If the attacker impersonates someone from inside the organization, then the attack can be called Business Email Compromise (BEC) (Federal Bureau of Investigation, 2021).

The motive behind a phishing attack varies. The intention of some attacks could be to acquire information from the target (Data entry) whereas in some attacks the intention could be to inject malware (Click only). If the intention is only to inject malware, a phisher could include a link to the email that directs the victim to a malicious website that automatically downloads malware to the computer making the user a victim by simply performing one click. (Jampen et al., 2022) (Sood & Zeadally, 2016). Phishing attacks that attempt to gather information, such as usernames, passwords, and credit card details, from a target, may include a link to a fake website that looks almost identical to a popular website like Gmail, Netflix, or a bank. Instead of downloading malware onto the victim's computer, the fake website typically presents a fake login page to trick the user

into entering their login credentials. By submitting their data, user becomes a victim of the phishing attack. (Parrish et al., 2009) (Hoxhunt, 2019)

Previous research provides some information regarding the differences in susceptibility to phishing attacks aimed at collecting credentials compared to phishing attacks designed to entice victims into visiting malicious websites that can automatically infect their computers with malware. In a study done by Rocha Flores et al. (2015) 9,2% of the participants clicked the phishing link, however only 4,9% manually executed malicious code. In a longitudional study by Lain et al. (2021) where they sent multiple phishing emails, 30% of participants clicked the phishing link once or more and 24% of the participants submitted their credentials on a phishing login page or enabled macros on the attached phishing document once or more. This thesis supports past research that users are less likely to further fall into the phishing attack if it requires a secondary action.

In this master's thesis, we found out that phishing attacks that try to collect login credentials (Data entry) are significantly less successful than phishing attacks that simply try to direct the victim to a malicious website (Click only). A total of five phishing emails with different characteristics were sent to approximately 86000 participants located in Nordic & Baltic countries. Half of the participants got *click only* phishing emails and the other half got *data entry* phishing emails. The success rate of *click only* phishing attacks was 45% whereas the success rate of *data entry* phishing attacks was only 16%.

English is a widely used language on the internet and most content on the internet on English (Web Technology Surveys, 2021) (Web Technology Surveys, 2023). Most phishing emails are also written in English (Simiou et al., 2020). Although English has traditionally been the dominant language used in phishing emails, this trend may be changing in some countries where most of the population does not speak English as their native language (Gendre, 2021) (Simiou et al., 2020). This exposes non-native English speakers (NNES) to a greater risk of becoming a victim of phishing if they are targeted in their native language rather than in English.

Previous research by Hasegawa et al. (2021) were able to find out with some level of certainty that phishing emails in local language would be more successful than phishing emails in English when the target is NNES. Their qualitative research was done by using online survey, and they had 862 NNES participants divided evenly in Germany, South Korea and Japan. One of the conclusions of this study was that participants in all countries felt that they would be more easily phished if the phishing email would be in their native language rather than in English. (Hasegawa et al., 2021).

To our knowledge, there have not been previous quantitative studies that focus on phishing susceptibility between English and a native language of a NNES using simulated phishing emails in an organizational environment. We argue that this master's thesis, which employs quantitative research methods and involves over 8,500 participants, confirms and strengthens the findings of the research conducted by Hasegawa et al. (2021). In this master's thesis, we discovered that participants were significantly more likely to fall victim to phishing attacks

when the email was written in their native language or the local language of their country, as opposed to English. This finding suggests that attackers who utilize the local language have a higher success rate in their phishing attempts.

Past research suggests that high proficiency in English is associated with a better ability to detect phishing emails written in English. This means that individuals with good skills in English are better at detecting phishing emails written in English than individuals with poor skills in English (Kävrestad et al., 2020). Our research supports this finding, as in Estonia the difference in susceptibility between the local language and the English language group was significantly lower compared to other countries. In Estonia, the proficiency level for English is high whereas in other countries in this study it is very high (EF, 2021). Denmark has the highest EF English Proficiency Index (EPI) score of 636, Norway, Sweden, Finland and Estonia have scores 632, 623, 618 and 581, respectively (EF, 2021).

Although, it is interesting that overall, our Norwegian participants were significantly the least successful at avoiding phishing emails while participants in Estonia were the most successful. We could not find any logical reason for these results. According to previous studies about phishing susceptibility rates for different demographics, young people and women are the most susceptible to phishing (Sheng;Holbrook;Kumaraguru;Cranor;& Downs, 2010), however, we didn't have significant differences regarding age between participants in Norway and Estonia. 24% of the participants in Norway and 20% of the participants in Estonia were aged 34 or less. There was a difference regarding gender between participants Norway and Estonia, however, the difference should've favored Norway. Only 23% of participants in Norway were female whereas 35% of participants in Estonia were female.

We found out that two of the five phishing emails were significantly more difficult to identify as phishing than the others. The commonality of these two phishing emails was that sender claimed to be some department in the organization. One of them being IT support and one being HR, both normally arguably trustworthy sources and having arguably high authority about the subject of the email. Otherwise, these two emails were not much alike. Two other emails were sent from outside of the organization from a person who was not known to the recipient and from one whose identity was unknown, and finally, one email was automatically drafter message from an IT system (printer). It seems users trust significantly more to emails coming from high authority, and inside the organization than from the outside. The fact that the email came allegedly from inside the organization probably boosted the authority cue. Usage of authority cues on phishing emails have been studied in the past as well, and these results support the findings of previous research (Williams, Hinds, & Joinson, 2018) (Moallem, 2019).

5.2 Weaknesses and limitations

Many of the participants in our study had received simulated phishing emails from their organization in the past, however, when we consider how big the organization is, we are certain that among our participants we had newly hired employees as well who hadn't yet gotten any simulated phishing emails from their organization. These participants' knowledge regarding phishing may have been worse compared to those who have been in the organization for a long time. We also didn't have any details regarding any of our participants' general IT skills or previous knowledge or experience regarding phishing emails, or how well they understood English. In theory, it is possible that in some groups we had more participants with advanced knowledge than in other groups.

Our study was purely quantitative, so we didn't know what kind of thought process the participant went through when they received the simulated phishing. For those that didn't succumb to phishing, we cannot be certain if the participant ever noticed the email or if they did a conscious decision to not click the link. For those participants that did succumb to phishing, we cannot be certain if the participant clicked the link knowing that it was only a simulated phishing email (and not real by an actual cybercriminal). Analyzing the email headers of the simulated phishing email, it was possible to identify that the email was sent from an anti-phishing training tool.

5.3 Practical implications

The organization, where this study was conducted, operates in countries where most of the population's native language is not English. The Cyber Security department of this organization has carried out anti-phishing training for their end users for multiple years. They have sent simulated phishing emails to the employees of the organization using both English and the local language of the specific country. The results of this study imply that the users of this organization are significantly more prone to succumb to phishing if the phishing email is written in the local language. If the organization wants to improve resiliency against phishing attacks it should send most (if not all) of the simulated phishing emails in the local language and highlight on other training material (like bulletins, emails, posters, etc.) the fact that cybercriminals can also use local language on their phishing campaigns.

Participants in this study clicked phishing links significantly more often than submitted their credentials on the fake login page. The organization should increase focus on training employees' ability to detect dangerous links on phishing emails and identifying the phishing attempt before clicking the link rather than focusing more on identifying fake login pages. Identifying fake login pages is still an important ability to learn since one can end up in fake login pages or

otherwise malicious websites while browsing the internet (Glover, 2023). Employees should also be made more aware of the reporting function that has been built in their email clients and to use it more often. Reporting the email using this function will send the email for technical analysis and later the user will get a statement whether the email is safe or not. This will help especially those users who are not entirely sure about the safety of the email and may be tempted to click the link to become certain.

In this study phishing emails that impersonated a department in the organization were significantly more successful than those that didn't thus this is yet another important factor for the organization to consider when making improvements to their anti-phishing training.

5.4 Future research

It's important to recognize the latest trends in phishing, including the language used in them, and use them in simulated phishing emails when training employees. The type of training and the interval of training is important as well. In this organization anti-phishing training mainly consist of awareness posters and few minutes long videos. This kind of passive learning is given approximately every three to four months. Future research should study if adding active learning alongside passive learning will have a positive impact for phishing resiliency. In the field of psychology, the importance of active learning and retrieval practice has already been studied (Roediger & Butler, 2010), however, not many studies in the field of information security and anti-phishing are to be found about this subject. There could be gap of knowledge between the two fields. Especially the information security field could greatly benefit the research done by psychologists since phishing uses psychological manipulation and phishing is arguably one the most used attacks against information systems and victims' digital data.

Qualitative research methods to further study users' behavior for all English emails, not just phishing, would probably benefit big multinational organizations. Past research has found out that users tend to ignore all emails that are written in English. This is a problem for multinational organizations. Some departments on these organization may have no other choice than to use English if they want to reach all relevant recipients. They may lack the time, skill, or resources to translate the message to all languages.

6 References

Abrams, L. (2022, September 20). *MFA Fatigue: Hackers' new favorite tactic in high-profile breaches.* Retrieved from https://www.bleepingcomputer.com/news/security/mfa-fatigue-hackers-new-favorite-tactic-in-high-profile-breaches/

Aldawood, H., & Skinner, G. (2019). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. *IEEE TALE Conference.* Wollongong: ResearchGate. doi:10.1109/TALE.2018.8615162

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science* (3). doi:doi.org/10.3389/fcomp.2021.563060

Anderson, R. (2020). *Security engineering: a guide to building dependable distributed systems.* John Wiley & Sons.

Arntz, P. (2017, January 20). *Understanding the basics of two-factor authentication.* Retrieved from https://www.malwarebytes.com/blog/news/2017/01/understanding-the-basics-of-two-factor-authentication

Baruch, M. (2016). *DGA detection using machine learning methods.* Jyväskylä: University of Jyväskylä. Retrieved from https://jyx.jyu.fi/handle/123456789/52755

Brecht, D. (2020, April 16). *Phishing techniques: Expired password/account.* Retrieved from https://resources.infosecinstitute.com/topic/phishing-techniques-expired-password-account/

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2015). Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails. *Australasian Conference on Information Systems*. Retrieved from https://arxiv.org/abs/1606.00887

Chen, J., Kakara, H., & Shoji, M. (2019). Operation ENDTRADE: TICK's Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data. Retrieved from https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

Collett, S. (2017). 5 reasons to take a fresh look your security policy: Evolving ransomware and DDoS attacks, new technology such as IoT, and changing user behavior are all good reasons to revise your security policy. *CSO (Online)*. Retrieved from https://search-proquest-com.ezproxy.jyu.fi/trade-journals/5-reasons-take-fresh-look-your-security-policy/docview/1922897782/se-2?accountid=11774

Conflict International (Director). (2017). *Hacking challenge at DEFCON* [Motion Picture]. Retrieved from https://www.youtube.com/watch?v=fHhNWAKw0bY

Digital And Population Data Services Agency. (n.d.). *Digital identity reform.* Retrieved from https://dvv.fi/en/digital-identity-reform

Doerfel, P., Thomas, K., Marincenko, M., Ranieri, J., Jiang, Y., Moscicki, A., & McCoy, D. (2019, May). Evaluating Login Challenges as a Defense Against Account Takeover. *WWW '19: The World Wide Web Conference*, 372–382. doi:https://doi.org/10.1145/3308558.3313481

DuoCircle. (n.d.). *Why You Need To Secure Your Emails With Email Gateway Services.* Retrieved from https://www.duocircle.com/content/email-gateway-service

EF. (2021). *A Ranking of 111 Countries and Regions by English Skilss.* Retrieved from https://www.ef.com/wwen/epi/

ENISA. (2011). *Botnets: Detection, Measurement, Disinfection & Defence.*

Federal Bureau of Investigation. (2021). *Internet Crime Report 2021.* Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Fruhlinger, J. (2020). Vishing explained: How voice phishing attacks scam victims. *CSO*. Retrieved from https://www.csoonline.com/article/3543771/vishing-explained-how-voice-phishing-attacks-scam-victims.html

Funkhouser, A. (2022, April 14). *Multi-Factor Authentication (MFA) Bypass Through Man-in-the-Middle Phishing Attacks.* Retrieved from https://www.netskope.com/blog/multi-factor-authentication-mfa-bypass-through-man-in-the-middle-phishing-attacks

Gatlan, S. (2022, June 6). Windows zero-day exploited in US local govt phishing attacks. Retrieved from https://www.bleepingcomputer.com/news/security/windows-zero-day-exploited-in-us-local-govt-phishing-attacks/

Gendre, A. (2021, February 21). The rise of non-English language spear phishing emails. Retrieved from https://www.helpnetsecurity.com/2021/02/26/non-english-spear-phishing-emails/

Gilbert, B. (2016, October 31). *Hillary Clinton's campaign got hacked by falling for the oldest trick in the book.* Retrieved from https://www.businessinsider.com/hillary-clinton-campaign-john-podesta-got-hacked-by-phishing-2016-10?r=US&IR=T

Global processing services. (2021, September). Sweden's journey to a cashless society. Retrieved from https://www.globalprocessing.com/news/blog/swedens-2023-cashless-goals

Glover, C. (2023, January 18). *Malvertising on Google Ads is a growing problem that isn't going away*. Retrieved from https://techmonitor.ai/technology/cybersecurity/malvertising-google-ads-malware

Goel, S., Williams, K., & Dincelli, E. (2017). Got Phished? Internet Security and Human Vulnerability. *Journal of the Association for Information Systems*(18), 22-44. doi:10.17705/1jais.00447

Goodman, S., Straub, D. W., & Baskerville, R. (2008). *Information Security: Policy, Processes, and Practices.*

Grimmick, R. (2022, June 16). *What is Cyber Espionage? Complete Guide with Protection Tips.* Retrieved from https://www.varonis.com/blog/what-is-cyber-espionage

Hasegawa, A., Yamashita, N., & Akiyama, M. (2021, August). Why They Ignore English Emails: The Challenges of Non-Native Speakers in Identifying Phishing Emails. *Proceedings of the Seventeenth USENIX Conference on Usable Privacy and Security* (pp. 319-338). USENIX Association.

Hong, J. (2012). The State Of Phishing Attacks. *Communications of the ACM*, 74-81. doi:10.1145/2063176.2063197

Hoxhunt. (2019, June 27). *Phishing 101: How Phishing Attacks and Scam Emails Work.* Retrieved from https://www.hoxhunt.com/blog/phishing-101-how-phishing-attacks-and-scam-emails-work

Hunt, T. (Director). (2019). *Ethical Hacking: Social Engineering* [Motion Picture]. Retrieved from https://app.pluralsight.com/library/courses/ethical-hacking-social-engineering/

Internet World Stats. (2019). *Internet world users by language*. Retrieved from https://www.internetworldstats.com/stats7.htm

Ives, B., & Learmonth, G. P. (1984). Information system as a competitive weapon. *Communications of the ACM*, 1193-1201. doi:doi.org/10.1145/2135.2137

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, 94-100. Retrieved from https://dl.acm.org/doi/10.1145/1290958.1290968

Jampen, D., Gür, G., Sutter, T., & Tellenback, B. (2022). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences*. doi:doi.org/10.1186/s13673-020-00237-7

Kaspersky. (n.d.). *What is Macro Virus?* Retrieved from https://www.kaspersky.com/resource-center/definitions/macro-virus

Keskin, S. (2022, May 24). 19 New E-Commerce Statistics You Need to Know in 2022. Retrieved from https://www.drip.com/blog/e-commerce-statistics#:~:text=In%202020%2C%20e%2Dcommerce%20sales,of%20all%20retail%20sales%20worldwide.&text=Notice%20the%20big%20jump%20from,and%2021.8%20percent%20in%202024.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: a real-world evaluation of anti-phishing training. *5th Symposium on Usable Privacy and Security* (pp. 1-12). Association for Computing Machinery. doi:10.1145/1572532.1572536.

Kävrestad, J., Pettersson, R., & Nohlberg, M. (2020). The language effect in phishing susceptibility. *Proceedings of the 6th International Workshop on Socio-Technical Perspective in IS Development (STPIS 2020) : Virtual Conference in Grenoble, France, June 8-9, 2020*, (pp. 162-167). Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-19355

Lain, D., Kostiainen, K., & Capkun, S. (2021). Phishing in Organizations: Findings from aLarge-Scale and Long-Term Study. *2022 IEEE Symposium on Security*

and Privacy (SP). Retrieved from https://dx.doi.org/10.1109/sp46214.2022.9833766

Lakshman, R. (2022, May 30). *Watch Out! Researchers Spot New Microsoft Office Zero-Day Exploit in the Wild.* Retrieved from https://thehackernews.com/2022/05/watch-out-researchers-spot-new.html

Lastdrager, E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science, 3*(9). doi:10.1186/s40163-014-0009-y

Limnéll, J. (2020). Jarno Limnéll | Mitä tapahtuu, kun koko elämäsi on kytköksissä internetiin? #72. (I. Rautio, & W. Von Der Pahlen, Interviewers) Retrieved from https://www.youtube.com/watch?v=1S5smvVAtlA&ab_channel=Futucast

MailGuard. (2021, August 5). *CREATIVES BEWARE: FILE SHARING SERVICE WETRANSFER USED IN FRESH PHISHING SCAM.* Retrieved from https://www.mailguard.com.au/blog/creatives-beware-file-sharing-service-wetransfer-used-in-fresh-phishing-scam

Mascellino, A. (2022, June 6). State-Backed Hacker Believed to Be Behind Follina Attacks on EU and US. Retrieved from https://www.infosecurity-magazine.com/news/statebacked-hacker-follina-attacks/

Maysh, J. (2016). The Man Who Sold the Eiffel Tower. Twice. *Smithsonian*. Retrieved from https://www.smithsonianmag.com/history/man-who-sold-eiffel-tower-twice-180958370/

Meskauskas, T. (2022, August 30). *How to avoid being scammed via the Dropbox phishing email.* Retrieved from https://www.pcrisk.com/removal-guides/18094-dropbox-email-scam#:~:text=What%20is%20%22Dropbox%20Email%20Scam,contained%20within%20another%20PDF%20document.

Microsoft. (2023, July 2). Trojans. Retrieved from https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/trojans-malware?view=o365-worldwide

Microsoft. (n.d.). *Mobile Authenticator App.* Retrieved from https://www.microsoft.com/en-us/security/mobile-authenticator-app

Moallem, A. (2019). *Human-Computer Interaction and Cybersecurity Handbook.* CRC Press.

Mohurle, S., & Patil, M. (2017). A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science, 8*. Retrieved from https://doi.org/10.26483/ijarcs.v8i5.4021

NETWORK, F. M. (Director). (2015). *Hacking challenge at DEFCON* [Motion Picture]. Retrieved from https://www.youtube.com/watch?v=fHhNWAKw0bY

Niemimaa, M., & Niemimaa, E. (2019). *Abductive innovations in information security policy development : an ethnographic study.* Taylor & Francis. doi:10.1080/0960085X.2019.1624141

Ohaua, C. (2006). Managing Phishing Threats in an Organization. *InfoSecCD '06: Proceedings of the 3rd annual conference on Information security curriculum development*, (pp. 159-161). doi:https://doi.org/10.1145/1231047.1231083

Om, K. (2017). Secure Email Gateway. *2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, (pp. 49-53).

Online Threat Alerts. (2018, July 20). "*Scanned from a Xerox Multifunction Printer*". Retrieved from https://www.onlinethreatalerts.com/article/2018/7/20/scam-scanned-from-a-xerox-multifunction-printer/

Parmar, B. (2012). Protecting against Spear Phishing. *Computer Fraud & Security*, 8-11. doi:10.1016/S1361-3723(12)70007-6

Parrish, J. L., Bailey, J. L., & Courtney, J. F. (2009). A Personality Based Model for Determining Susceptibility to Phishing Attacks.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment.* Edinburgh: Command, Control, Communications and Intelligence Division.

Pew Research Center. (2021). *Social Media Fact Sheet.* Retrieved from https://www.pewresearch.org/internet/fact-sheet/social-media/

Proofpoint. (2019). *Human factor report.* Proofpoint. Retrieved from https://www.proofpoint.com/us/resources/webinars/human-factor-2019

Raggad, B. (2010). *Information Security Management: Concepts and Practice.* Taylor & Francis Group.

Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., & Duezguen, R. (2020). An investigation of phishing awareness and education over time: When and how to best remind users. *Sixteenth Symposium on Usable Privacy and Security.* The advanced computing systems association. Retrieved from https://www.usenix.org/conference/soups2020/presentation/reinheimer

Renaud, K., Reinheimer, B., Rack, P., Ghiglieri, M., Mayer, P., Kunz, A., & Gerber, N. (2018). Developing and Evaluating a Five Minute Phishing Awareness Video. *TrustBus 2018: Trust, Privacy and Security in Digital Business*, (pp. 119-134). doi:10.1007/978-3-319-98385-1_9

Rocha Flores, W., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information & Computer Security, 23*(2), 178-199. Retrieved from https://doi.org/10.1108/ICS-05-2014-0029

Roediger, H. L., & Butler, A. C. (2010, October 18). The critical role of retrieval practice in long-term retention. *Trends in Cognitive Sciences*. doi:doi.org/10.1016/j.tics.2010.09.003

Rosenthal, M. (2022). *Must-Know Phishing Statistics: Updated 2022.* Retrieved from https://www.tessian.com/blog/phishing-statistics-2020/

Rublon. (2022, April 20). *What Is SMS 2FA? Text Message Authentication Explained.* Retrieved from https://rublon.com/blog/what-is-sms-2fa/

Satter, R. (2017). Inside story: How Russians hacked the Democrats' emails. *Associated press*. Retrieved from https://apnews.com/article/dea73efc01594839957c3c9a6c962b8a

Schober, P., & Vetter, T. R. (2018). Repeated Measures Designs and Analysis of Longitudinal Data: If at First You Do Not Success - Try, Try Again. *Anesthesia and analgesia, 127*, 569–575. Retrieved from https://doi.org/10.1213/ANE.0000000000003511

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). *Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions.* doi:10.1145/1753326.1753383

Sheng, S., Wardman, B., Warner, G., Cranor, L. F., Hong, J., & Zhang, C. (2009). *An Empirical Analysis of Phishing Blacklists.*

Simiou, C., Zand, A., Thomas, K., & Bursztein, E. (2020). Who is targeted by email-based phishing and malware? Measuring factors that differentiate risk. *In Proceedings of the ACM Internet Measurement Conference (IMC '20).* doi:https://doi.org/10.1145/3419394.3423617

Sood, A. K., & Zeadally, S. (2016, September 28). Drive-By Download Attacks: A Comparative Study. *IT Professional, 18*(5), 18-25. doi:10.1109/MITP.2016.85

Stanton, B., Theofanos, M. F., Prettyman, S., & Furman, S. (2016). Security Fatigue. *IT Professional*, 26-32. doi:10.1109/MITP.2016.84

Särökaari, N. (2020). *Phishing attacks and mitigation tactics.* Jyväskylä: University of Jyväskylä. Retrieved from https://jyx.jyu.fi/handle/123456789/72569

Tenzer, H., Pudelko, M., & Harzing, A.-W. (2014). The impact of language barriers on trust formation in multinational teams. *Journal of International Business Studies*(45), 508-535. doi:10.1057/jibs.2013.64

Thurman, M. (2003). Security policies? What security policies? *Computerworld*, 32. Retrieved from https://search-proquest-com.ezproxy.jyu.fi/trade-journals/security-policies-what/docview/216090448/se-2?accountid=11774

US Fed News Service. (2009). Beware of Text Message Spam: 'Smishing'. *US Fed News Service*. Retrieved from https://search-proquest-com.ezproxy.jyu.fi/newspapers/beware-text-message-spam-smishing/docview/472725071/se-2?accountid=11774

US Fed News Service. (2010). SMISHING: PHISHING BY CELL PHONE TEXTS. *US Fed News Service*. Retrieved from https://search-proquest-com.ezproxy.jyu.fi/newspapers/smishing-phishing-cell-phone-texts/docview/471956905/se-2?accountid=11774

Warner, E. (2021, November 17). *How Law Firms Can Avoid Phishing Scams in 2022*. Retrieved from https://www.eversparkinteractive.com/blog/law-firm-phishing-scams-dont-get-hooked/

Web Technology Surveys. (2021, November 12). *Usage statistics of content languages for websites*. Retrieved from https://archive.ph/20211112133335/https://w3techs.com/technologies/overview/content_language#selection-551.0-551.50

Web Technology Surveys. (2023, January 22). *Usage statistics of content languages for websites*. Retrieved from https://w3techs.com/technologies/overview/content_language

Weinberg, N. (2013, March 6). *How to blunt spear phishing attacks*. Retrieved from https://www.networkworld.com/article/2164139/how-to-blunt-spear-phishing-attacks.html

Wikileaks. (n.d.). Retrieved from https://wikileaks.org/podesta-emails/emailid/34899

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 1-13.

Witts, J. (2022, March 1). *What are Email Security Gateways, How Do They Work, and What Can They Offer Your Organization?* Retrieved from https://expertinsights.com/insights/what-are-email-security-gateways-how-do-they-work-and-what-can-they-offer-your-organization/

Wright, R., & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems*.

Xero. (2022). *Reporting Phishing to Xero.* Retrieved from https://www.xero.com/blog/security-noticeboard/