Miku Airaksinen

MASTER'S THESIS

THE STATE OF PHISHING – AN ANALYSIS ON THE INDICATORS OF PHISHING ATTACKS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

ABSTRACT

Airaksinen, Miku
The State of Phishing – An Analysis on the Indicators of Phishing Attacks
Jyväskylä: University of Jyväskylä, 2022, 68 pp.
Cyber Security, Master's thesis
Supervisor: Vuorinen, Jukka

The goal of this thesis was to analyze the contents of phishing communications and determine the features within those communications that can be recognized as indicators of phishing by the users that receive the communications. This thesis was heavily influenced by the largely established notion of users being the weak link of information security. It was because of this idea that the approach of this thesis was focused on the common users that are generally not deeply knowledgeable on information security matters. The focus on how common users evaluate the communications also led to the idea of developing an experimental framework for recognizing phishing communications as such by evaluating user context by analyzing contextual phishing indicators.

The research was conducted by collecting a sample of different phishing communications that utilize various attack vectors. These communications were then analyzed by using the developed experimental framework to discover the rate of occurrence of different social, technical, and contextual indicators within each phishing communication.

The results of the research suggest that factors related to user context can be highly significant phishing indicators. This is still merely a preliminary finding that demands more research. It was also shown that a prominent trend within phishing websites is that the websites are most often perfect or nearly perfect fabrications of legitimate websites, which can make it difficult for users to recognize them as phishing sites. Lastly, the results of this thesis indicate that the set of indicators found in each attack can vary depending on which attack vector is utilized in the attack.

Keywords: Phishing, Social Engineering, Information Security, Context, Indicator

TIIVISTELMÄ

Airaksinen, Miku
The State of Phishing – An Analysis on the Indicators of Phishing Attacks
Jyväskylä: Jyväskylän yliopisto, 2022, 68 s.
Kyberturvallisuus, Pro Gradu -tutkielma
Ohjaaja: Vuorinen, Jukka

Tämän Pro Gradu -tutkielman tavoitteena oli analysoida kalasteluviestinnän sisältöä ja määritellä ne viestinnän piirteet, jotka viestinnän vastaanottava käyttäjä pystyy tunnistamaan kalastelun indikaattoreiksi. Tätä työtä ohjasi laajalti hyväksytty ajatus siitä, että käyttäjä on tietoturvallisuuden heikoin lenkki. Tämän vuoksi työ keskittyikin tarkastelemaan viestintää nimenomaan sellaisten tavanomaisten käyttäjien näkökulmasta, jotka eivät ole erityisen perehtyneitä tietoturvallisuuteen. Tämä rajaus johti myös siihen, että työtä varteen kehitettiin kokeellinen viitekehys, jonka avulla viestintää arvioitiin käyttäjän kontekstin näkökulmasta tarkastelemalla viestinnässä ilmeneviä kontekstuaalisia kalastelun indikaattoreita.

Tutkimus toteutettiin keräämällä otos erilaisista kalasteluhyökkäyksistä jotka hyödyntävät erilaisia hyökkäysvektoreita. Näitä hyökkäyksiä analysoitiin työtä varten luodulla viitekehyksellä, jotta eri hyökkäyksien sisältämien sosiaalisten-, teknisten- ja kontekstuaalisten indikaattoreiden määrät saatiin selvitettyä.

Tutkimuksen tulokset osoittavat, että käyttäjäkontekstiin liittyvät tekijät voivat toimia merkittävinä kalasteluindikaattoreina. Tämä on kuitenkin vain alustava löydös, jota pitää tutkia lisää. Tutkimuksessa osoitettiin myös se, että kalastelusivuilla ilmenevä merkittävä trendi on se, että sivut ovat useimmiten täydellisiä tai lähes täydellisiä väärennöksiä aidoista verkkosivuista. Tämä voi johtaa siihen, että käyttäjillä voi olla vaikeuksia tunnistaa sivustot kalastelusivuiksi. Lopuksi, tämän tutkielman tulokset viittaavat siihen, että kalasteluhyökkäyksissä ilmenevät indikaattorit voivat vaihdella merkittävästi riippuen siitä, mitä hyökkäysvektoria hyökkäyksessä käytetään.

Asiasanat: Tietojen kalastelu, Social engineering, Tietoturvallisuus, Konteksti, Indikaattori

FIGURES

TABLES

SISÄLLYS

1 INTRODUCTION

Phishing is a type of cyberattack that is also a form of social engineering. Its purpose is to get access to sensitive information that is otherwise not accessible by posing as a trustworthy actor via electronic communication (Myers & Jakobsson, 2007, 1). Phishing as a modern concept is believed to have surfaced around 1996. At the time, several American Online (AOL) accounts were stolen through the means of phishing passwords from the users of AOL (San Martino & Perramon, 2010, 164).

Phishing presents a major threat to all kinds of organizations, especially those that are in possession of large amounts of sensitive information. San Martino and Perramon (2010, 165) reference the findings of PhishTank, suggesting an average of 10,000 monthly phishing scams between 2006 and 2008. Rader and Rahman (2015, 23) bring up the reports of the Anti-phishing Working Group (APWG). According to them, the number of phishing attacks rose tremendously between 2010 and 2012, with the number of attacks going from approximately 50,000 attacks during the first half of 2010, to approximately 120,000 attacks during the second half of 2012. The growth of the number of phishing attacks can be seen in figures 1 and 2.

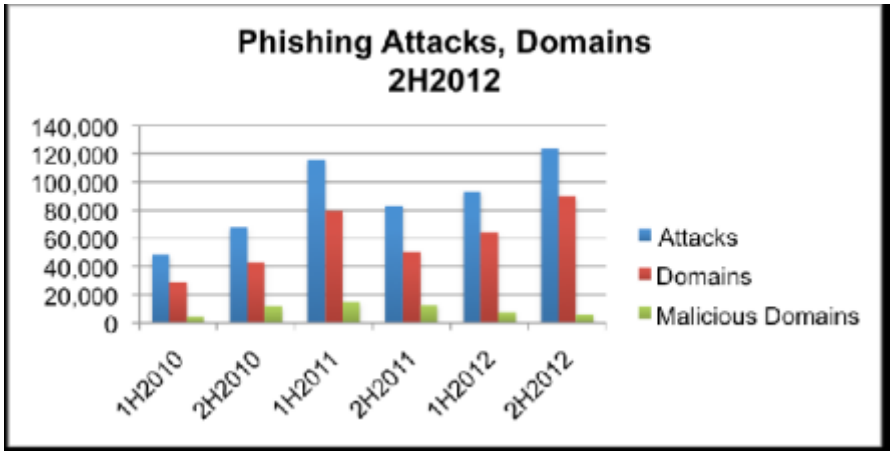


Figure 1: Phishing attacks (APWG, 2013)

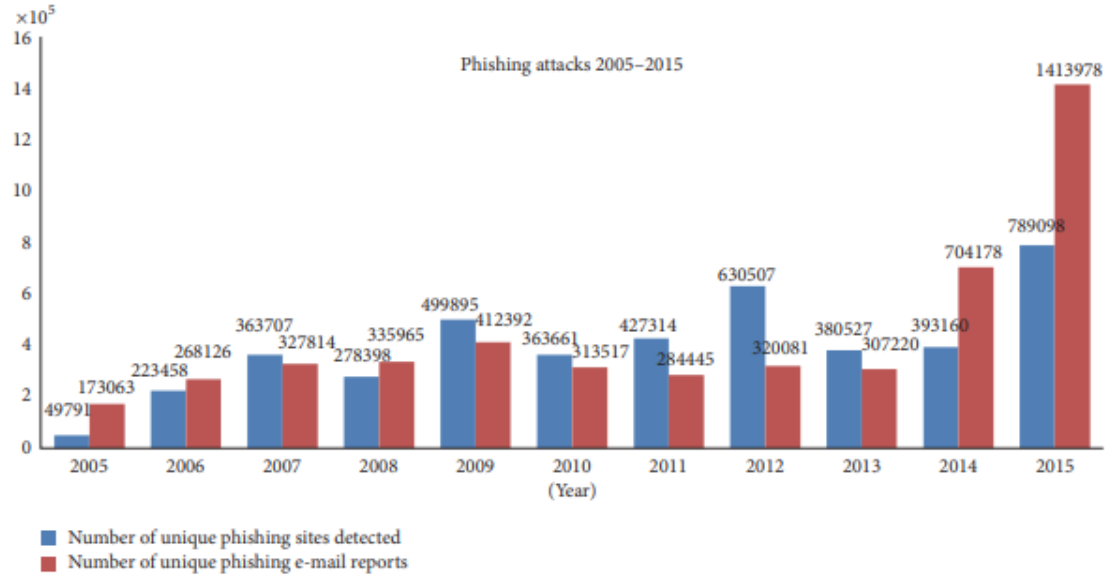


Figure 2: Phishing growth by 2005-2015 (Jain & Gupta, 2017, 3)

The impacts of phishing attacks can be profound. San Martino and Perramon (2010, 165) refer to Gartner's report, stating that each phishing incident costs around 900 USD. Jain and Gupta (2017, 2) claim a total number of approximately 450000 phishing attacks in 2013 which led to more than 5.9 billion dollars in financial losses. APWG (2017) reported at least 255,065 unique phishing attacks worldwide in 2016, which is a 10% increase over 2015. While different sources may report differing numbers, it seems clear that phishing attacks have been increasing over the years. With the increase in the number of phishing attacks over the years, the estimated overall costs caused by phishing attacks are also on the rise.

The necessity of this thesis is based on two primary factors. Firstly, based on the aforementioned research results, it is evident that phishing is a major threat facing both organizations and common people. Efforts need to be made to attain a better understanding of how phishing works, to be able to provide better tools for users so that phishing attacks can be avoided.

Secondly, and most importantly, a thorough literature review on social engineering research suggests that something is missing. Tetri and Vuorinen (2013, 1018) touched on this issue, suggesting that previous analysis approaches have lacked in utilizing explicit underlying theories, and that the approaches of SE research should be based on analyzing multiple dimensions simultaneously. The key factor here is that of context. Tetri and Vuorinen argued that it is important to consider the wider context surrounding phishing attacks. The notion of context being an important piece of the puzzle makes sense, but it also needs to be confirmed through other literature.

1.1 Research question

With an established understanding of the impact and status of phishing attacks, and a vague notion of understanding that something is potentially missing from current SE research, the importance of this thesis is evident.

Although a multidimensional approach concerning SE research is important, it is also vital to maintain clear boundaries on what will be researched. Social engineering is a grand subject that demands plenty of research. This thesis cannot do it all, but it can be one piece of the puzzle. As discussed previously, a major premise of this thesis is based on the importance of analyzing the wider context in phishing attacks. However, researching nothing but context in phishing attacks could lead to an overly difficult to conduct research that does not necessarily provide any relevant findings on its own.

Information security practitioners and researchers have widely accepted a consensus on users being the weak link of information security (see e.g. Thomason, 2013, Hughes-Lartey, Li, Botchey & Qin, 2021, Yan et. al, 2018). This notion further dictates the focus of this thesis on the actions and thought processes of the users. If the users are indeed the weak link of information security, it also stands to reason that improving the information security performance of users can decrease the likelihood of phishing attacks being successful. A baseline for the research question of this thesis should thus be that it needs to be related to the factors of the attack that influence the user. Additionally, this thesis is seeking to confirm the previously mentioned notion of the importance of context in analyzing phishing attacks.

These established baselines lead to a set of research problems that this research seeks to solve. Firstly, this thesis seeks to discover how context relates to phishing attacks. This problem, on its own, is too open-ended, and needs further limitations to serve as a research question. Further limitations concerning the research questions are based on this thesis having a focus on what the user sees and does, and that it is based on the notion of the user being the weak link. Previous research indicates that there are specific cues that can be recognized as indicators of phishing attacks. Lastly, it is important to ensure that this research utilizes previous knowledge on social engineering while also analyzing recent data to ensure the relevance of the research. These limitations and baselines thus lead to the following three primary research questions:

- Are there contextual indicators of phishing attacks that the common user can recognize?
- What are the most common indicators of phishing attacks that the common user can recognize?
- What is the frequency of different indicators recognizable by common users in recent phishing attacks?

Here, a common user refers to someone who is not an information security specialist. Those who are knowledgeable on information security matters will

already be able to avoid most, and hopefully all, phishing attacks. The pool of users mainly consists of those who are not specifically knowledgeable on information security matters. Thus, it is important to limit the research so that the focus is on those who are the most vulnerable. The research is also very specifically limited on discussing indicators that can be recognized by common users. Naturally, with enough training, even a common user could recognize deeply technical indicators of phishing attacks. However, most common users will never receive phishing training of this depth. Thus, it is more meaningful to focus efforts on understanding indicators that can be recognized with little or no training at all.

Security specialists and educators can utilize the results of this research by developing training materials that are based on the established common characteristics of phishing attacks. The focus of this thesis will be limited on the human side of phishing attacks, mainly the interactions of the user and what the user sees when encountering a phishing message.

1.2 Research methodology

A sufficient base of knowledge will have to be established by conducting a thorough literature review before anything else. Knopf (2006, 127) discusses literature reviews, stating their beneficial goals as giving a general overview of a body of research, revealing what has already been done well, giving new ideas for research, determining the problems and flaws of previous research, and enabling the placement of a research project in a larger context to be able to show potential new conclusions that could result from said research project. The purpose of the literature review in this thesis is to serve as both a theoretical frame of reference in the later stages of the research, and to answer the first two research questions. There is a vast amount of previous research on social engineering and phishing. These research do not come without their issues, but they will be able to direct the research in the right direction as well as serve as a sufficient base of knowledge for the purposes of this thesis.

A portion of the literature review that stands out on its own as a major part of the theoretical frame of reference is frame analysis theory. Frame analysis is a term initially introduced by Erving Goffman in 1974. Goffman (1986, 1-2) explains the concept of frame analysis as a way in which people draw meaning to matters, a way of analyzing social realities. In relation to social engineering, there are two crucial factors that highlight the significance of frame analysis. Firstly, it serves as a core part of how users evaluate the phishing messages presented to them and generally how they draw an understanding of their reality. Secondly, in his work, Goffman (1986, 83) discusses fabrications and how users are made to believe that a specific subject is something that it is not. This knowledge serves as a basis for understanding some of the differences between factual messages and fabricated messages, and specifically the differences in how the users process these messages.

The basis of Goffman's (1986, 10-11) frame analysis theory begins with the concept of frames. In relation to frame analysis, frames are the basic element of frame analysis. Frames are known as specific situations, such as a man and a woman kissing. According to Goffman, definitions of a situation are based on the principles of organization that govern events, as well as the subjective involvement of an individual. Thus, frame analysis can be defined as the way in which individuals evaluate the situation in combination with their contextual knowledge. In practice, this indicates that a man and a woman kissing can be several things, such as a couple kissing, a man greeting his wife, or something else, all depending on the entire base of knowledge regarding the situation and its context. A lot depends on who is analyzing the frame. A child might have a very different outlook on the situation than an adult might. Johnston (1995, 217) summarizes the definition of frames by referring to the definitions suggested by Gamson, Fireman and Rytina in 1982 that refer to frames as mental orientations that organize perception and interpretation.

Goffman (1986, 21) states that when an individual draws meaning to an event, they employ one or more frameworks that can be called primary. The frameworks are called primary due to them not depending on a prior interpretation of a situation. A primary framework renders meaning into otherwise meaningless aspects of a scene. A primary framework allows an individual to locate, perceive, identify, and label concrete occurrences. Goffman also states that to draw meaning to specific situations, there are usually several frameworks that are employed to understand the situation.

Goffman (1986, 22) separates primary frameworks into two classes: natural and social. Natural frameworks are also referred to as unguided events: events that are, from start to finish, dictated by natural determinants. An example of a natural framework is the weather. The second class of primary frameworks, the social class, is of more relevance to this thesis. The purpose of social frameworks is to provide background for events that incorporate the will, aim, and controlling effort of another individual or a group of individuals. In a manner of speaking, these classes can be considered to be on two sides of a spectrum in terms of the degree of guidance. Natural frameworks are unguided, while social frameworks are guided events.

Other essential factors in frame analysis are keys and keyings. Goffman (1986, 43-44) starts by defining keys as the set of conventions by which an already meaningful activity (given its meaning by a primary framework) is transformed into something else. The process of this transformation is called keying. Goffman (1986, 45) defines keying as a process in which a systematic transformation is applied on subjects that are already meaningful in terms of a primary framework. Those participating in the transformation process are meant to know and acknowledge the ongoing systematic transformation. There are cues available for knowing when the transformation starts and when it ends. Keying is not restricted to any class of perspectives. And finally, the systematic transformation that occurs within keying may only slightly alter the activity happening, but the individual's interpretation of the activity can be utterly changed.

As established, keying is a way of transforming an activity into something else, with all relevant parties understanding that a transformation is taking place. Goffman (1986, 83) discusses another method of transformation, fabrication. Goffman defines fabrication as "the intentional effort of one or more individuals to manage activity so that a party of one or more others will be induced to have a false belief about what it is that is going on". Goffman suggests that some level of malicious intent is involved in fabrication. In relation to fabrications, Goffman names those who develop the deception as operatives, fabricators, or deceivers. Those who are the target of the fabrication can be called the dupes, marks, or victims, to name a few examples. As previously established, within this thesis, the targets of the fabrication will be called users.

The essential difference between keying and fabrication is the degree of involvement. Goffman (1986, 84) states that the communication pertaining to fabrications is collusive: there are those who are in on it that communicate collusively, and then there are those who are not in on it, who are being colluded against. This brings us to the very heart of social engineering: an operative or a group of operatives developing a setting that a target individual or a group of individuals considers legitimate and then acts according to the supposedly correct norms concerning the fabricated setting.

Frame analysis provides a theoretical understanding of how individuals draw meaning to matters. This knowledge will serve as a basis for evaluating how users view phishing messages, and what are the keys needed for recognizing the messages as fabricated. As previously mentioned, this thesis seeks to identify indicators of phishing attacks. Essentially, indicators in phishing are what keys are in frame analysis. They serve as the variable that transform an act into something else entirely.

Frame analysis provides a suitable theoretical base for this thesis to systematically analyze phishing attacks. This leads to the empirical section of this thesis. The third research question of this thesis demands analysis that has not been previously conducted. The goal is to analyze recent phishing attacks to evaluate the frequency of different indicators recognizable by common users. The basis of analyzing each example phishing attack will be on first identifying the frames and the keys of each attack. With the frames and keys of the phishing attacks established, the keys can be related to the common indicators that will be established further on in the literature review of this thesis.

The relation of keys to the established indicators is, essentially, the data collection phase of this thesis, that will provide the answer to the third research question of this thesis, the frequency of different indicators in phishing attacks. Frequencies will be determined not just for the frequency of appearance of single indicators, but for a combination of indicators as well, meaning that when analyzing the frequency of indicators, efforts will be made to determine if there are connections between the appearance of specific groups of indicators: whether there are some indicators that often make appearances with other indicators.

As this research seeks to determine the frequency of different phishing indicators in recent phishing attacks, the data collection and analysis phases are

classified to be quantitative. Goertzen (2017, 12-13) defines quantitative research methods as methods that that are used to collect and analyze data that is structured and can be represented numerically. Quantitative research methods are effective in answering questions such as "what" and "how", e.g: "What percentage?", "What proportion?", "How many?" or "How much?". Goertzen states the advantages of quantitative research to be the generalizability of findings to a specific population, data sets being large and thus representative of a population, documentation regarding the research framework and methods being shareable and replicable, and finally, standardized approaches allowing for the replication of the study over time. The limitations, according to Goertzen, are that quantitative data does not provide evidence for why populations think, feel or act in certain ways, certain population groups being difficult to reach, and studies sometimes being time consuming and requiring data collection over long periods of time.

The methodology of this thesis is likely not to suffer from the disadvantages of quantitative research. The literature review will evaluate several previous social engineering research to have a better understanding of why users act in certain ways regarding phishing messages. Inferences will be made based on the analysis of previous data. Additionally, previously developed theories that are based on previous findings of SE research can also be utilized. Goertzen also brought up a disadvantage of quantitative research being the difficulty of reaching specific population groups. While this disadvantage does not directly apply to this thesis, a minor challenge can be identified as a by-product: attaining a dataset that is diverse and large enough, so that the results can be generalized.

Collecting a suitable set of data is not the only challenge within the development of this thesis. Suitable statistical analysis methods also need to be determined. According to Singleton and Straits (2018, 501), statistics has been divided according to two functions, descriptive and inferential. The purpose of descriptive statistics is focused on organizing and summarizing the data to make it easier to interpret. Inferential statistics concern making inferences when generalizing from data. The empirical section of this thesis only seeks to answer a basic question concerning the frequency of specific indicators in a data set. Based on these definitions and the general setting of this thesis, descriptive statistics is a valid approach and will thus be used.

Having established an idea of the necessity of SE research as well the research questions of this thesis and the methodology that will be used to collect and analyze data, the next two sections seek to develop a clear image of what social engineering and phishing are. The next section will be focused on discussing the fundamentals of social engineering and phishing, their history and the current issues relating to the respective research fields. Afterwards, discussion will move to dissecting phishing attacks in-depth.

2 ON SOCIAL ENGINEERING AND PHISHING

To better understand phishing, it is essential to first look at social engineering. Hadnagy and Fincher (2015, 53-71) define it as an act of consciously guiding another person's choices. According to them, a social engineer's actions could be considered beneficial or malicious, depending on their intentions. Influence and manipulation are concepts that are pivotal to social engineering. Alexander, Podgorecki and Shields (1996, 1) define social engineering as the process of "arranging and channelling environmental and social forces to create a high probability that effective social action will occur".

Alexander, Podgorecki and Shields (1996, 3) claim that the greatest social engineers of the twentieth century were political dictators such as Lenin, Stalin, and Hitler. While these dictators have been known to sway people by exploiting feelings of fear and authority, their rule cannot be classified as a type of social engineering. Their use of violence as a method of ruling separates them from social engineers. The key difference that separates dictators from modern social engineers is the degree of subtleness. Dictators can be very direct in utilizing fear as a tool, and their subjects will likely be aware of how they are being influenced. The targets of successful social engineering attacks, on the other hand, will not be aware of the attacks and do not understand that they are being influenced.

According to Workman (2007, 315), the goal of social engineering is to manipulate people into performing actions or sharing confidential information. The attained confidential information such as driver's licenses can then be sold at a black market.

As stated by Rader and Rahman (2015, 27-28) as well as Workman (2007, 316), social engineers target and manipulate human emotions such as curiosity, excitement, fear, and empathy. Chaudhry, Chaudhry, and Rittenhouse (2016, 250) also discuss the techniques that social engineers use to trick users. Curiosity, fear, and empathy are the key emotions that are taken advantage of during phishing attacks. People desire to stay informed. This feeling of curiosity can be exploited by sending a link to watch the latest news stories, for example. The link then leads the user to a malicious website. Feelings of fear can also be exploited by posing as a legitimate authority such as a bank and informing the user that their bank

account may have to be frozen unless the user performs a specific action, likely one that leads to the user divulging their personal information such as login credentials to the attacker. Empathy can also be exploited by posing as a friend or a relative, or by exploiting a tragedy such as a natural disaster and asking for help.

2.1 What is phishing?

Phishing is a type of cyberattack that exploits a significant weakness in information security, human behavior. Jakobsson and Myers (2007, 1) define it as a form of social engineering, the purpose of which is to claim sensitive information from the target organization by posing as a trustworthy actor via electronic communication. Hadnagy and Fincher (2015, 2) define it simply as the practice of sending e-mails that appear to be from trustworthy sources with the goal of attaining personal information or influencing the target of the attack to do something.

James (2005, 7-8) refers to phishing as a form of spam in which phishers represent themselves as legitimate companies, with the intention of acquiring sensitive information. James (2005, 38) continues by suggesting one popular method that phishers utilize to be impersonation, which is a method of deceit that is composed of a fake website that the user is tricked into visiting.

Phishing can be classified as a type of attack that requires both social and technical understanding. Typically, a phishing attack consists of three components: the lure, the hook, and the catch**,** in that order. The lure is what first gets the attention of the victim, most commonly an email message that appears to be from a legitimate source such as a bank. The message contains a link to the hook. The hook is a website that is a copy of the legitimate source's (such as a bank) website. A successful hook gets the user to divulge their personal information to the illegitimate website. The catch is the final phase of the phish, in which the attacker makes use of the collected information (Chaudhry et al., 2016, 249).

Phishing attacks incur costs that are both direct and indirect. The direct costs alone can be severe, depending on what type of target the attack is made on. For example, The Gartner Group claimed a combined cost of $1.2 billion in phishing fraud related damages in the year 2004 alone. Phishing attacks also cause reputational damage to the targeted organizations, which can lead to losing business opportunities, which in turn leads to financial losses (Jakobsson & Myers, 2007 4-5). Phishing attacks are also highly effective. Their effectiveness has led to a demand for technical anti-phishing solutions (Ludl, McAllister, Kirda and Kruegel, 2007, 20). While technical solutions are valuable, it is the purpose of this research to focus on the elements of phishing that are visible to the target of the phishing attack.

2.2 History of phishing and social engineering

The history of social engineering dates to the times of ancient Greece and the siege of Troy. The well-known ploy of bringing a Trojan horse (that was used to hide Greek soldiers) inside the city walls was devised by a Greek by the name of Sinon (Rader and Rahman, 2015, 24).

The birth of phishing can be dated back to 1996 and the theft of several American Online (AOL) accounts. The term phishing is based on the analogy that the thieves used email as a fishing hook to "phish" for sensitive information. (San Martino & Perramon, 2010, 164). Grobler (2010, 1) states that "Ph" is a common hacker replacement for the letter "f". Grobler also refers to the theft of AOL accounts as being the first recorded mention of the term "phishing". According to Grobler, after this event, phishers would often use email requests to attain sensitive information. Quite often these emails would be littered with spelling errors. Grobler as well as Rader and Rahman (2015, 25) consider the origin of the term "phishing" to stem from the word "phreaking". According to Rader and Rahman, phreaking is the hacking of phone networks that allowed a person to make free phone calls by blowing a toy whistle into the phone.

Grobler (2010, 1) states that phishing had evolved to a more sophisticated level in 2003, with the use of techniques such as look-alike domain names, fake websites that had started to look legitimate and proper language, among other things. Jakobsson and Myers (2007, 23-24) also highlight the advancement of phishing attacks, stating that in the beginning the lures of the attacks were easy to distinguish as bait, and the imitation websites were crude. Since then, the attacks have made several advancements that have polished the phishing attacks, partly due to the division of labor in the phishing community.

2.3 Issues with previous and future research

There is a plethora of issues and contradictions concerning previous research on phishing and social engineering, which will be discussed in the coming sections. The purpose of the discussion is to highlight the problems within the field of SE research, and then propose solutions to these problems in relation to the scope of this thesis.

2.3.1 Defining phishing

One of the concerns of social engineering and phishing research is that of the definition of phishing. Some sources, such as Herath, Chen, Vishwanath, and Rao (2012, 1) as well as Hadnagy and Fincher (2015, 2) suggest that phishing is a scam that is based on utilizing e-mail as the primary attack vector. Other sources such as Yeboah-Boateng and Amanor (2014, 297) refer to different forms of phishing as well, such as SMS phishing (or SMiShing) that uses SMS messages as the attack

vector, or Vishing (voice phishing), that uses phone calls as the attack vector. Hadnagy and Fincher (2015, 5-6) consider vishing to be an assistive technique that is used to follow up on e-mails sent by phishers.

Besides the utilized attack vectors, another essential element of phishing is the matter of fake websites developed for the purpose of attaining sensitive information. These websites can either be considered a step of the attack process of a common phishing attack (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2007, 2) or an attack vector by themselves (Banu and Banu, 2013, 783) or an attack vector in conjunction with search engine phishing (Chaudhry, Chaudhry, and Rittenhouse, 2016, 251) (Howard & Komili, 2010, 2).

Going forward, a clear definition is necessary. While there are several research results that indicate e-mail being the most popular attack vector, it is certainly not the only vector. Even if most attacks do utilize e-mail, discussing phishing as only or primarily an e-mail-based attack may serve as a distraction, shifting the attention away from other potential attack vectors. The same attack could also use a combination of two or more attack vectors to make the messaging seem more legitimate. Previous findings indicating e-mail being the sole vector could potentially be explained by a change in the field of phishing: e-mail may have been the sole attack vector, but the field has since then expanded to utilize SMS or other instant messaging platforms, social media, and phone calls, as supportive or primary vectors.

A broad definition can now be suggested for the purposes of this thesis. Phishing is a type of cyberattack that targets users, with the goal of attaining sensitive information, gaining access to information systems, or influencing the target to do something else. Phishers utilize one or more technical or social tricks to make the user believe the message to be legitimate. Phishing attacks can utilize one or more attack vectors to target the user.

2.3.2 Focus of social engineering research

In the earlier discussions, a consideration of Tetri and Vuorinen (2013, 1014) was presented. The consideration is, that within the field of SE research, the existing findings and discussions show a scattered and vague collective understanding of what the building blocks of social engineering are. Tetri and Vuorinen also suggested that the current field of SE research is overly focused on analyzing individual differences relating to how users evaluate the messages they receive, as well as on the persuasion techniques that the attackers use. Arguments can be made for why research should focus on these aspects, but this approach is problematic in that it leaves other factors that can have an influence on the success of SE attacks out of consideration.

Current analysis on SE literature suggests that the field is still suffering from similar issues. The impact of these issues on this thesis is minimal. The goal of this thesis is not to develop or validate an all-encompassing SE framework. Instead, the focus here, like on several other research works before this, is on the building blocks of phishing attacks. There will be no definitive analysis on what

makes a phishing attack successful. The interest is on attaining an understanding of what recent phishing attacks look like.

The limitations of previous research on SE, while having a minimal impact on this thesis, do still have an impact. As outlined earlier, when discussing potential indicators of phishing attacks, heavy considerations will be given to the role of context in determining whether a message is legitimate or a phishing attack. This focus on context does not come without issues. For example, when analyzing phishing messages, it will be difficult, and likely impossible, to reliably determine potential contextual indicators that relate to the user receiving the message. Another issue here is, as mentioned earlier, that the significance of context has not been widely discussed in previous research works.

There is not a large amount of readily available information pertaining to context within the domain of social engineering. Determining contextual factors when analyzing recent phishing messages will be extremely difficult, at least within the scope of this thesis. This results in a clear limitation that this thesis will face. Determining the contextual indicators will be largely based on collecting a set of generalized inferences from previous works and other findings that point towards contextual indicators. The legitimacy of contextual indicators cannot be determined within the scope of this thesis. The suggested contextual indicators can, however, serve as a starting point for future research.

2.3.3 Ethics

Social engineering research is faced by another essential issue, which is that of ethics. Research data on social engineering is scarce. This can be partly explained with the ethical demands of research. Mouton, Malan, Kimppa and Venter (2015, 2) discuss the ethical issues of social engineering in detail. One such issue is that social engineering attacks may have unintended after-effects on the victim. Mouton et al. mention that social engineers take advantage of human nature by getting the users to disclose information that they do not necessarily understand the importance of. Social engineering attacks are a seemingly vile and personal type of attack that, in a manner of speaking, intrudes a user's personal space quite harshly.

Mouton et al. (2015, 7) consider social engineering research to be an environment in which research subjects are exposed to social engineering attacks and social engineering awareness tests. In some cases, the research subjects are not informed of their participation in advance, so that their awareness of the research does not alter their actions, which could potentially lead to inaccuracies in the research results.

Hatfield (2019, 359) notes that attaining consent can cause an ethical dilemma in penetration testing. Jones, Towse and Race (2015, 24-25) reference previous studies which implicate that it is important for the research subjects not to know that they are being researched, so that they do not alter their actions due to knowing that they are being researched. Jones et al. also highlight the importance of both voluntary participation as well as remaining sensitive, especially when working with past fraud victims. Finally, Jones et al. also mark the importance of

immediately debriefing research participants when they are subjected to a social engineering attack.

In summary, social engineering research faces numerous ethical concerns that need to be addressed to ensure the ethicalness of the research. To avoid any issues, receiving informed consent for performing the research is a necessity. However, in the case of informed consent, receiving it poses an issue: how to ensure that the research subject does not alter their actions, knowing that they are being researched. A research subject could well be more alert simply knowing that they will be targeted. This, in turn, means that they are not acting as they normally would, meaning that the results of the research would be less representative of how the subject would normally act, leading to inaccuracies in the results. Jones et al. (2015, 25) suggest an approach in which research participants are informed that they will be receiving a phishing e-mail in the future. This way, participants are giving informed consent, but will have potentially forgotten that they have signed up for the study in the first place, leading to them reacting to the phishing e-mail in the same as they normally would.

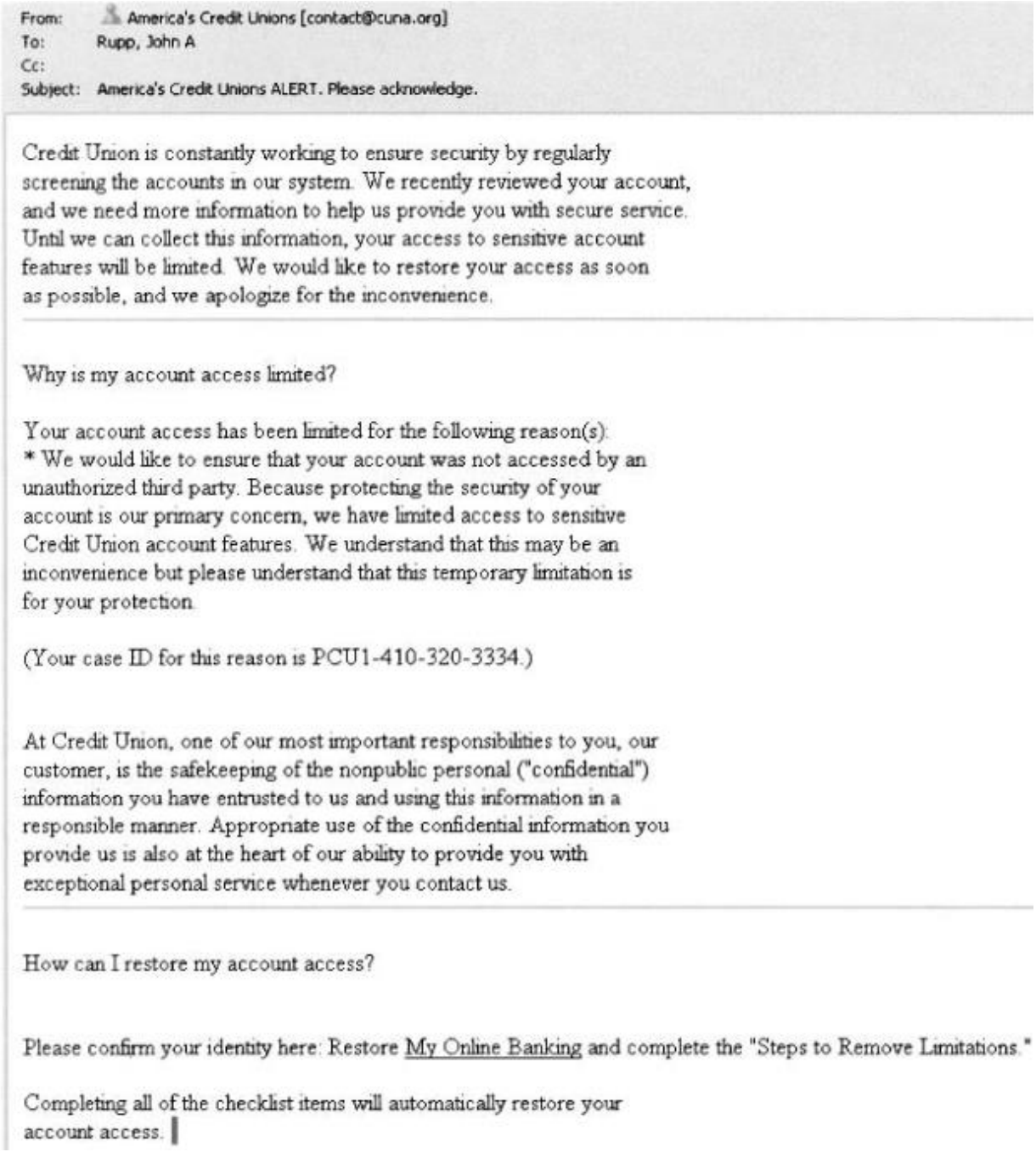
Another concern that needs to be addressed is that of debriefing. Research participants that are subjected to a social engineering attack need to be debriefed immediately after the results of the attack have been observed, for the purposes of educating the user and ensuring that the user does not feel traumatized after the attack (Jones et al., 2015, 25) (Mouton et al., 2015, 12-14). Finally, Jones et al. (2015, 24) also suggest that some level of deception in the form of withholding information from the research participants is necessary when performing social engineering research to attain results that are as accurate as possible.

The impact of ethical demands of research on this thesis are minimal. The analysis of phishing messages is conducted on real attacks that have already taken place and thus does not lead to users being exposed to anything new. There are two primary takeaways concerning research ethics for the purposes of this thesis. Firstly, when analyzing phishing attacks, efforts need to be made to ensure that the anonymity of the victims is maintained. Secondly, existing data needs to be evaluated through an understanding of the limitations of social engineering research. If the used research methods have been entirely ethical, there is a possibility of the results being tainted due to the users knowing that they will be attacked.

3 DISSECTING PHISHING ATTACKS

Figures 3, 4 and 5 serve as prime examples of what a typical user might see when opening a phishing message or when entering a malicious website. Even at the very first glance of these pictures, an experienced user will likely recognize them as phishing attacks. Recognizing a message as phishing is one thing, but it is potentially even more important to be able to understand what makes them phishing messages. In the upcoming sections, several references will be made back to these three figures, that serve as key examples of phishing attacks and will allow for analysis of their common features.

After analyzing previous literature on social engineering and phishing, 3 basic buildings blocks of phishing attacks were identified that form the basis of what a phishing attack is made of. Figure 6 shows a phishing attack dissected into its core features. The key to this figure, especially pertaining to this thesis, are the different domains of indicators. What are the indicators that will lead the user to recognize the messages as fraudulent? This knowledge will allow the user to have a better chance of avoiding falling for more advanced phishing attacks. In the upcoming sections, we will dissect example phishing attacks by first building an understanding of the common features of phishing messages and then discussing how these features appear in the example attacks.



From: America's Credit Unions [contact@cuna.org]
To: Rupp, John A
Cc:
Subject: America's Credit Unions ALERT. Please acknowledge.

Credit Union is constantly working to ensure security by regularly screening the accounts in our system. We recently reviewed your account, and we need more information to help us provide you with secure service. Until we can collect this information, your access to sensitive account features will be limited. We would like to restore your access as soon as possible, and we apologize for the inconvenience.

Why is my account access limited?

Your account access has been limited for the following reason(s):
* We would like to ensure that your account was not accessed by an unauthorized third party. Because protecting the security of your account is our primary concern, we have limited access to sensitive Credit Union account features. We understand that this may be an inconvenience but please understand that this temporary limitation is for your protection.

(Your case ID for this reason is PCU1-410-320-3334.)

At Credit Union, one of our most important responsibilities to you, our customer, is the safekeeping of the nonpublic personal ("confidential") information you have entrusted to us and using this information in a responsible manner. Appropriate use of the confidential information you provide us is also at the heart of our ability to provide you with exceptional personal service whenever you contact us.

How can I restore my account access?

Please confirm your identity here: Restore My Online Banking and complete the "Steps to Remove Limitations."

Completing all of the checklist items will automatically restore your account access.

Figure 3: A Typical phishing e-mail (Jakobsson & Myers, 2007, 7)

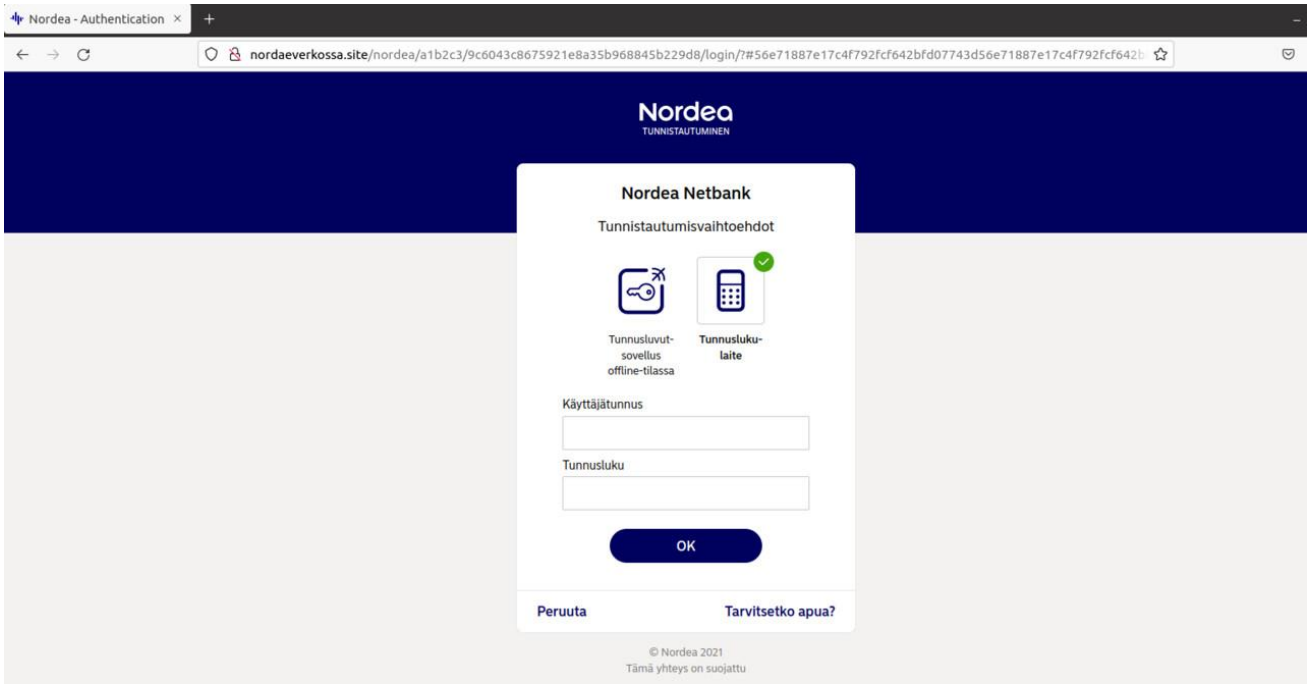


Figure 4: Fake Nordea Domain (National Cyber Security Centre, 2021)

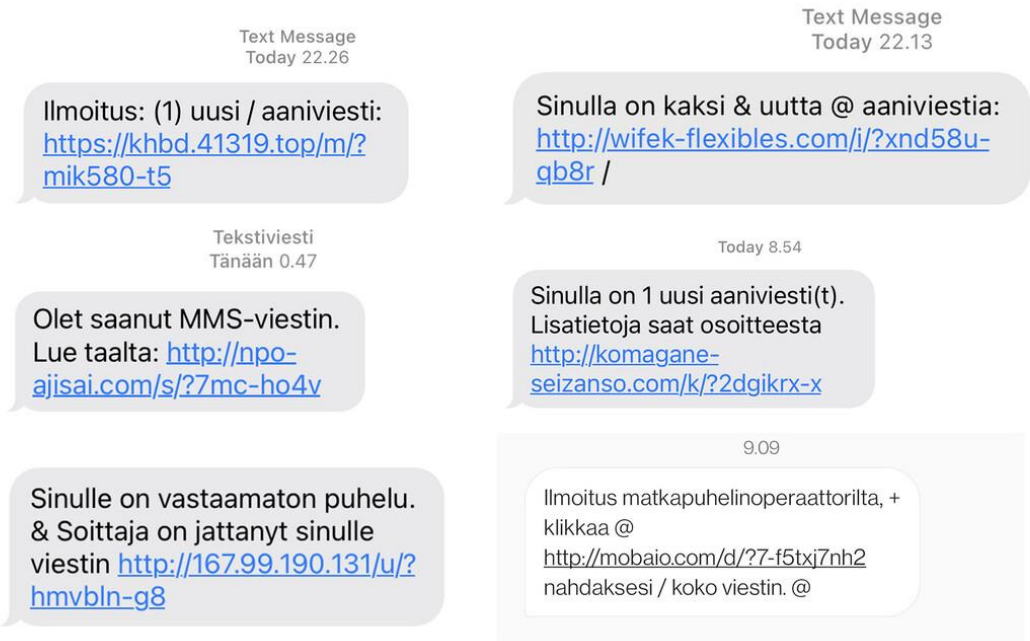


Figure 5: Scam text messages (National Cyber Security Centre, 2021)

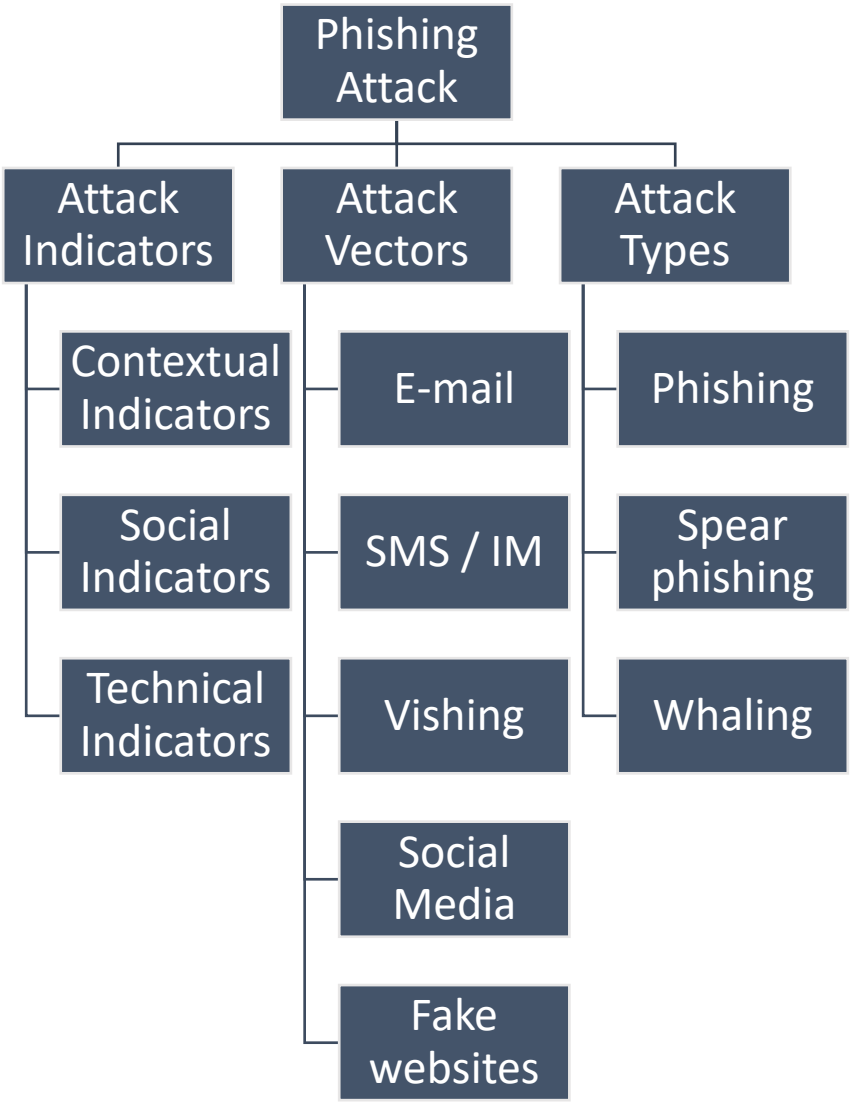


Figure 6: The building blocks of a phishing attack

3.1 Attack indicators

This section is dedicated to discussing the previously mentioned key part of figure 6: the attack indicators. Attack indicators, in previous literature, are roughly split into two categories: technical and social. After discussing these two categories of indicators, a third possibility of indicators will be presented: contextual indicators.

3.1.1 Technical indicators

Figure 7 is a presentation of common technical phishing indicators, which will be discussed in detail within this section. Jakobsson and Myers (2007, 65) categorize

spoofing into three different categories that are relevant to phishing: Email spoofing, IP spoofing and web spoofing. In addition to these three categories, caller ID spoofing is also a relevant technique that is used in vishing, which is a form of phishing attack explained further on. This leaves us four separate spoofing categories that are relevant to this thesis.

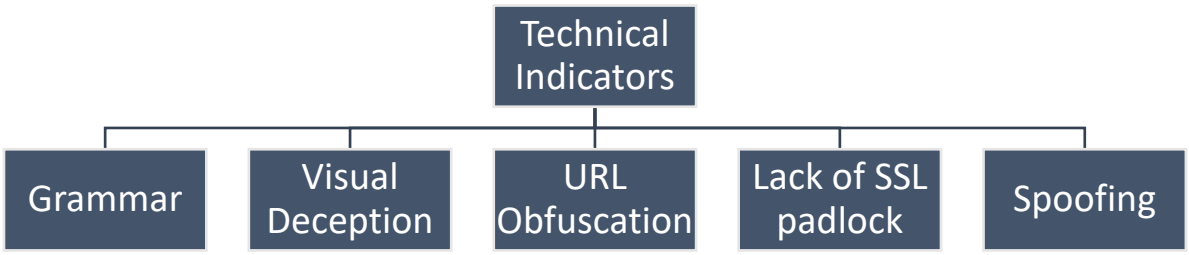


Figure 7: Technical Indicators

Song, Kim and Gkelias (2014, 865) define caller ID spoofing as a technique that changes the number of the incoming call that is displayed on the phone screen. Deng, Wang, and Peng (2018, 369) refer to it as forging the authentic caller's identity, thus making it appear as though the call is originating from another user. According to them, it is a technique that is easy to perform and hard to detect.

E-mail spoofing is a technique that makes the source of the email appear to be different than what it is. It is highly common, with almost every internet user today likely having witnessed it in one form or another (Jakobsson and Myers, 2007, 65). According to Hadnagy and Fincher (2015, 4), in e-mail spoofing the information in the "From" section of the e-mail is falsified. The source is changed to make it look like it is sent by someone that the user knows or a trustworthy source such as a cable company.

IP spoofing is what is known to be the act of modifying an IP packet by replacing its actual source address with a fake one. IP spoofing is a technique that is utilized in several different cyberattacks, such as man-in-the-middle, distributed denial of service attacks and DNS poisoning attacks (Vlajic, Chowdhury and Litoiu, 2019, 1). According to Ali, (2007, 3) most IP spoofing is done for illegitimate purposes, such as attackers wanting to hide their own identity. IP spoofing can be done by using tools such as hping and sendip or others that are available for free on the internet.

Figure 3 shows a simple example of what E-mail spoofing could look like. In this message, the attacker has falsified the "From"-section to make it seem as if the message has originated from America's Credit Unions, with the e-mail address of the sender being contact@cuna.org. Despite the limited information available concerning America's Credit Unions, some assumptions can be made based on the available open sources. To start off, a quick google search shows that the supposed name of the organization in question is in fact America's Credit Union, not America's Credit Unions. This small error is already a minor red flag.

Let's have a further look at the e-mail address. The domain used in the message is @cuna.org. Browsing to the website of America's Credit Union's "Contact Us" -page (N.d.), we will find that the e-mail address of the organization's Mortgage Department ends in @youracu.org. Thus, the official e-mail domain name of America's Credit Union is entirely different from the one in the phishing message. Further google browsing on the @cuna.org brings us to the website of Credit Union National Association, the website of which is cuna.org. However, as was the case with America's Credit Union's website, accessing the "Contact Us" -page of Credit Union National Association (N.d.), we will find that the e-mail domain in use for contact is @cuna.coop.

This analysis does leave some room for error. An obvious issue here is that the picture was presented as a source by Jakobsson and Myers in 2007, which means that the message dates back to at least 2007, if not further. This means that the website and e-mail domains currently in use can be entirely different from what they were in 2007. Another issue of our analysis is that google searches concerning America's Credit Union led us to two different websites of seemingly two different organizations with the same name. An organization could also have multiple different e-mail domains in use. Finally, this analysis also serves as an indication of how difficult it can be to evaluate the legitimacy of a message based on the e-mail address alone. This suggested difficulty indicates that the legitimacy of messages should be evaluated using multiple domains of indicators.

Moving on from the analysis of e-mail spoofing, there is still one more domain of spoofing to be discussed, which is one of the most essential spoofing techniques: web spoofing. Web spoofing is just one of the many ways used to refer to fake websites, that are an essential part of most phishing attacks. The goal of phishing attacks is not just to get the user to click a malicious link in a phishing message, but to also believe the website that the link leads to is legitimate, and then out some of their personal information to the fake site.

According to Banu and Banu (2013, 785), web spoofing is utilized by a phisher to create a website that looks identical to a legitimate website. The purpose of web spoofing is to get the user to enter their personal information such as login credentials to the fake website, that the attacker then collects. Grobler (2010) refers to web spoofing as not so much an assistive technique but as something that happens every time in phishing attacks, stating that "phishers use various techniques to trick users into accessing their fake website", implying that most, if not all phishing attacks share the same goal of getting the user to access a fake website. Banu and Banu (2013, 783) also suggest that the fake websites might redirect the user to the legitimate website after they have typed in some of their personal information, so that it would seem to the user as if nothing out of the ordinary happened. Thus, they would likely not even be aware of having just been under attack.

Hadnagy and Fincher (2015, 4) refer to fake websites simply as website cloning. According to them, in website cloning "scammers copy legitimate websites to fool you into entering personally identifiable information (PII) or login credentials".

Brody, Mulig and Kimball (2007, 47-48) discuss pharming, which is based on utilizing fake, imitated websites in combination with technologically advanced techniques. They suggest pharming to be a form of phishing in which the attacker has implanted a malicious program on the target computer. When the user types in a legitimate web address in a browser, the user is taken to a fake website that is visually an imitation. Jakobsson and Myers (2007, 105-123) define pharming as an assistive technology that phishers use. It is a method that utilizes vulnerabilities in the DNS software which allow the attacker to redirect web traffic from one website to another.

Attackers can increase the visit rates of fake websites by utilizing a technique called search engine phishing. It is a technique in which phishers take advantage of search engine functionalities to get the fake websites to show in users' search results. Should the user enter the illegitimate website, the phishing attack works similarly from that point onwards as with other forms of phishing. The user may end up typing in some of their personal information (Chaudhry, Chaudhry, and Rittenhouse, 2016, 251). Search engine phishing is based on a technique called search engine optimization (SEO), which is commonly used by organizations to boost the amount of visits their websites get. While initially the goals of SEO have been focused on developing legitimate businesses, SEO can also be used for malicious purposes, such as guiding user traffic to malicious websites that are used to phish personal information or distribute malware (Howard & Komili, 2010, 2). SEO is about manipulating search engines by using things such as meta tags, content, graphics, and keywords to improve site rankings (Ledford, 2015, 19).

Another technique phishers can take advantage of is URL obfuscation. Grobler (2010) defines URL obfuscation as disguising "URLs to trick the target into connecting to the phisher's proxy server and not the real server. Grobler continues the subject of URL obfuscation by explaining some of the different techniques for performing URL obfuscation. Phishers can purposefully register and use "bad domain names", the purpose of which is to be similarly named as a trusted source such as a legitimate bank. Attackers can also utilize friendly login URLs, which are supported by some web browser implementations. This allows for URLs to include authentication information such as a login name and password. Attackers can also utilize third-party services to shorten URLs to obfuscate the destination of the link. Lastly, attackers can use host name obfuscation by navigating to a website using an IP address.

Garera, Provos, Chew and Rubin (2007, 2) continue the subject of categorization of different types of URL obfuscation, suggesting 4 types of obfuscation:

1. Type I: Obfuscating the host with an IP address
    a. In type 1, the URL hostname is replaced with an IP address
2. Type II: Obfuscating the host with another domain
    a. In type 2, the URL's host contains a valid looking domain name, and the path contains the organization being attacked
3. Type III: Obfuscating with large host names

   a. In this type, the organization being phished is in the host, but there is a large string of words and domains after the host name
4. Type IV: Domain unknown or misspelled
   a. In the fourth type there is no apparent relationship to the organization being phished or the domain name is misspelled

According to analysis provided through google safe browsing toolbar in 2006, type III is the most popular type of URL obfuscation, followed by type I, with the percentage of attacks being 46.46% and 33.32%, respectively. Type II comes third, with 17.30%, and type IV with 2.9% (Garera et. al., 2007, 5).

URL obfuscation is a seemingly common technique in phishing attacks that can be used in conjuncture with a fake website to make the user feel more at ease when entering personal information. Examples of URL obfuscation have been shown in reports by the Finnish National Cyber Security Centre in 2021, pictures of which are found in figures 4 and 5.

Figure 4 shows a fraudulent version of Nordea's service for identification. It serves as an example of both URL obfuscation as well as what a copied fake website could look like. The key takeaway here is that it is nearly identical to Nordea's actual identification site. Those who have used Nordea's services would likely not immediately recognize any difference from the official site. The fraudulent website is nearly identical to the official one. The key factor here is the URL address that can be seen in the address bar. The URL reads as "nordaeverkossa.site…". Here, we can identify that the name of the domain is misspelled while also being made to look believable at first glance. The Finnish National Cyber Security Centre (2021) reported that this malicious identification website was used in a campaign in which attackers pretended to contact people in the name of My Kanta Pages and the Suomi.fi service, with the goal of phishing for banking details.

Figure 5 shows various examples of scam text messages that were used as a part of a malware campaign called FluBot. In this example, several types of URL obfuscation are present. For example, the message at the bottom left of the figure has obfuscated the host by masking it with an IP address instead of the domain name (National Cyber Security Centre, 2021).

Phishing attacks can use trademarks, logos and images that are associated with the suggested source organization to make the message / website seem more trustworthy (Chaudhry, Chaudhry, and Rittenhouse, 2016, 250). These are factors that can be categorized into tricks that are based on visual deception. In addition to using legitimate logos, visual deception techniques can include text that is visually deceptive, such as substituting letters in domain names that are easy to go unnoticed, for example www.paypal.com using the number "1" instead of the letter "l". A common technique phishers use is an image of a legitimate hyperlink, while the image itself is a hyperlink to another website altogether. Websites can also utilize images mimicking browser windows or dialog windows. Finally, visually deceptive techniques can include an illegitimate browser window being placed next to a legitimate browser window, leading to

the user potentially believing that both windows are legitimate (Dhamija, Tygar and Hearst, 2006, 584).

Techniques that can be categorized as visual deception can be found in figures 3 and 4. In the e-mail presented in figure 3, the sender is presented as America's Credit Unions, while the organization's supposed name is likely America's Credit Union, as discussed previously. The fake website presented in figure 4 uses visual deception techniques more openly. It uses Nordea's logos and other visual trademarks exactly as Nordea does. The website is a nearly identical copy of the actual identification site. There is a clear overlap with techniques related to fake websites, as visual deception techniques are an essential part of developing the copied websites.

One of the common characteristics of a phishing attack is the language containing anomalies. There can be minor matters such as occasional weird capitalizations or other issues (Hadnagy & Fincher, 2015, 5). In some cases, the tone of the language, misspellings or unprofessional design can be the only clues of a phishing attack. (Dhamija, Tygar and Hearst, 2006, 584). The language of phishing messages is often formal (Grobler, 2010, 2).

Formal language can be seen in the examples presented previously in figures 3 and 4. Despite this, in figure 3 there are some minor grammatical issues that serve as indicators of a phishing message. For example, the subject line contains the word 'ALERT' fully in upper case letters. This seems like it strays from official sounding, grammatically correct language. In the middle of the message, the sentence "(Your case ID for this reason is PCU1-410-320-3334.)" raises suspicion. On one hand, a case ID for an issue such as this is in line with what communication of this kind could look like. On the other hand, the word 'reason' stands out as incorrect. A seemingly better word could have been 'ticket' or 'issue'.

The grammatical errors found in the scam text messages in figure 5 are clearer than in figure 3. Three of these Finnish text messages use the word 'Ääniviesti' (Voice message), but the Umlauts in 'Ä' are not spelled out. The umlauts are missing from other words that should use them as well. The messages also use special characters such as '&' and '@' in seemingly odd places that don't fit with the rest of the message.

Vishwanath, Herath, Chen, Wang and Rao (2011, 579-583) suggest that when users were targeted with phishing attacks, the level of attention paid to the source of the e-mail as well as to the grammar and spelling of the e-mail would be negatively correlated to the user's likelihood to respond to the e-mail. Additionally, Vishwanath et al. discovered that the level of attention paid to the subject line was positively related to the individual's likelihood to respond to the phishing e-mail. These results indicate that grammar and spelling mistakes can serve as indicators of phishing messages, and e-mail source as well as subject lines could also contain indicators of phishing attacks.

Wang, Herath, Chen, Vishwanath and Rao 's (2012, 349) findings also suggest that grammatical errors are indicators of phishing messages. According to them, grammatical issues often appear in phishing emails. Additionally, the

authors also discuss spoofed sender's addresses, which are another indicator of phishing messages. Their findings also indicate that users commonly pay attention particularly on grammar and spelling when determining the legitimacy of an email.

There are several other technical security indicators pertaining to user performance that may suggest a phishing attack, whether it is a website, e-mail, or some other platform for delivering the phishing message. One key security indicator is the SSL closed padlock found on the left side of the browser address bar. Users may often simply scan the website for a closed padlock regardless of its position. Thus, a closed padlock icon in a different position than usual may fool the user into believing that they are browsing securely (Dhamija, Tygar and Hearst, 2006, 584). The fake website built to look like Nordea's identification site presented in figure 4 shows an example of this. The not closed SSL padlock icon in the address bar indicates that the site is not secure. A common user could potentially trust this website due to the message at the bottom, which says "Tämä yhteys on suojattu", which translates to "This connection is secure" or "This connection is protected". This text is also found at the bottom of Nordea's actual identification website.

Irani, Webb, Giffin & Pu (2008, 3) discuss the anatomy of phishing messages. According to them, phishing messages can be split into two components: the content and the headers. The content is the part of the message that the user sees. It is used to deceive the user. The headers are the parts of the message that are primarily used by the mail servers and the mail client. Their purpose is to "determine where the message is going and how to unpack the message".

Irani et. al. (2008, 7) continue discussing the features of phishing messages, dividing the features into two groups: transitory features and pervasive features. Transitory features have a relatively small lifespan and only appear in a small number of attacks. Pervasive features are the opposite of transitory features in terms of the number of appearances, appearing in a relatively larger number of attacks.

According to Irani et. al. (2008, 8), in addition to the division between transitory features and pervasive features, phishing features in messages can be broadly split into four groups:

1. Header features
    a. Header features refer to anything concerning the headers of the messages
2. Content features
    a. Content features refer to anything concerning the content of the messages
3. URL features
    a. URL features refer to anything concerning the utilization of URL features in phishing messages
4. Meta features
    a. Meta features represent a combination of header features, content features or URL features

Bhardwaj et. al. (2020, 18-19) also discuss common technical features and unique tactics of phishing messages and phishing sites, shown below in table 1. Some of these features, such as the shortening service or abnormal URLs are the kind that the user can see and react to, while others like the HTTPS token & port or google index are the kinds of features not directly visible to the common user.

Phishing Features	Description
Content embedding	Images, video, contents implanted in phishing page & sharing the same domain.
Shortening service	To hide the spoofed URL, a shortening service redirects to the phishing page.
@ symbol	Alphanumeric characters are ignored after the @ symbol.
- prefix or suffix	Adding a prefix or suffix separated by a '-' indicates phishing subdomains.
Length of URL	Spoofed subdomains or long URLs are used to hide the spoofed phishing sites.
IP address	Use of an IP Address instead of the spoofed URL.
Double '.'	Phishing sites typically have more than one '.' Subdomain URLs
HTTPS token & port	Use of HTTPS token and non-standard ports (8081, 8090…) indicates phishing.
Double slash redirection	Use of '//' in URL for redirection.
No Google index or rank	Phishing websites do not have Google indexing or rank.
Popup windows	Phishing sites usually open popup windows, seeking user submissions.
Mouseover disabled	Mouseover() command is kept disabled so URL cannot be seen by end users.
Rightclick disabled	Rightclick() function is disabled for most phishing pages.
Abnormal URLs	Use of non-standard and abnormal URLs instead of original host domain.
Domain age	Phishing sites are newly hosted domains and do not last long.

Table 1: Features for phishing detection (Bhardwaj et. al., 2020, 19)

3.1.2 Social indicators

Based on previous research such as Chaudhry, Chaudhry, and Rittenhouse (2016, 250), Ferreira, Coventry and Lenzini (2015, 39-41) Rader and Rahman (2015, 27-28) and Workman (2007, 316), the key emotions (shown in figure 6) taken advantage of in phishing attacks are in no specific order of importance:

- Fear
- Curiosity
- Empathy
- Greed

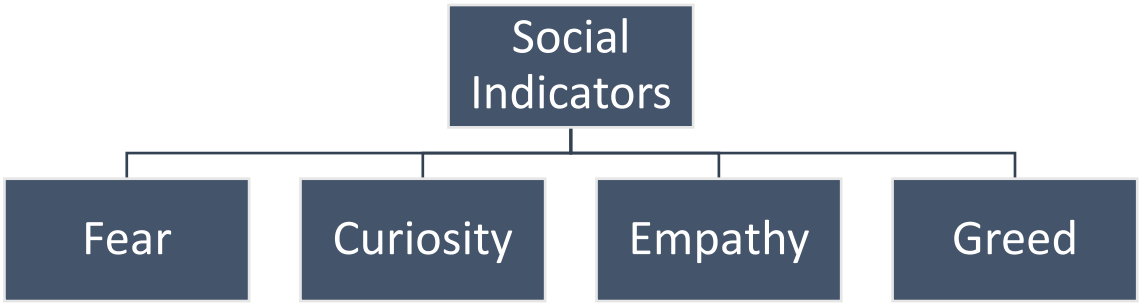


Figure 8: Social Indicators

Feelings of fear are exploited by making the user believe that they have done something wrong, or that they must immediately do something to make sure that they do not lose access to something important, for example their bank account (see e.g., Chaudhry et. al., 2016, 250 & Jakobsson, 2016, 31). Some sources, such as Ferreira, Coventry and Lenzini (2015, 42-44) discuss the exploitation of authority being a major tool in social engineering attacks. Authority often relates to fear due to the contents of the authoritative messages. An example of this can be seen in figure 3, where an authoritative source (a credit union) tells the user that their access to their services has been limited due to the credit union suspecting that the user's account was accessed by an unauthorized source. Due to this authoritative message, the user may fear for their account's security. Authority, while being a major method of influencing users, can be seen as one domain of fear, when discussing social engineering attacks.

Phishers take advantage of the natural urge of people to stay informed, relating to feelings of curiosity (Chaudhry et. al., 2016, 250). An example of exploiting feelings of curiosity can be seen in the phishing text messages presented in figure 5, in which the user is urged to listen to or read a message they have supposedly received. If humans do indeed have a natural urge to stay informed, then these messages may have the desired effect, as the user would be interested to find out the contents of the message.

Feelings of empathy are utilized to get the user to do something that the user thinks is being done for a friend or a relative, or someone in dire need of help (Chaudhry et. al., 2016, 250). The exploitation of empathy relates to the presentation of other people's actions. Feelings of empathy can be exploited by referring to other people (that the user may already know) being familiar with the author of the message. This may lead to the user lowering their guard and feeling safe with the author of the message. Empathy is also exploited in the sense that phishing messages often try to exploit the natural willingness of people wanting to help others, and their tendency to believe what others say and need. Phishers also try to make the messages seem more relatable to users by using falsified information to make the contents of the message, the author, or suggested actions of other seem real. (Ferreira et al., 2015, 42-44). An example of this could be a message in which the author presents themselves as a system

administrator from the same company the user works at, asking the user to test a link. Another similar example is that of a friend asking the user to visit a website that seems interesting. (Jakobsson, 2016, 31). If the user were to believe the author to be working in the same company as they are, it makes sense that they would also be more inclined to trust them.

Finally, exploiting the feeling of greed is another major way of influencing users. When influenced with greed, people focus on one thing and ignore other things (Ferreira et. al., 2015, 40). In this case, when feelings of greed are exploited, the users are focused on something they can gain, such as money, and they miss the fact that they are likely being scammed. Figure 3 shows an example that exploits feelings of fear and authority as well as greed. In the message, the user is informed that their account access is limited. The user may feel that the supposed actions taken by the message author takes something away from the user (as it would if the message was real). The user may thus become overly focused on losing access to services that they previously had access to, and ignore other things pertaining to the message, such as indicators of an attack.

One of the social indicators that have not been previously discussed are urgency cues. Vishwanath et al. (2011, 579-583) found that the likelihood of users responding to a phishing message is positively related to the level of attention paid to the urgency cues. Urgency cues are loosely connected to Cialdini's (2006) principle of scarcity, in which the influencer attempts to persuade the target by means of referring to the uniqueness of what they are offering. Urgency cues function similarly, suggesting that what is being offered should be accepted urgently to ensure that nothing is lost. Williams, Hinds and Joinson (2018, 1-2) discuss the impact of urgency cues, suggesting that urgency influencing techniques exploit the limited time employees have to process information to get them to act against their best interests by taking time away from the decision-making process. Urgency influencing techniques are largely dependent on the specific work context. In some contexts, the employees may have more time for processing information than in others.

It was also similarly found that users who pay an overly large amount of attention on visceral triggers (urgency cues, in this case) were more likely to respond to a phishing e-mail. It was also found that that paying attention to deception indicators would make it less likely that the user would respond to a phishing message (Wang et al., 2012, 354-355).

The findings of both Vishwanath et al. (2011) and Wang et al. (2012) do show that the level of attention paid on urgency cues increases the likelihood of the user responding to a phishing e-mail. However, it is the view of this author that this finding is not as simple as it would at first seem to be. Wang et al. (2012, 348) base their take concerning urgency cues on previous studies which suggest that urgency cues would raise a sense of exigency in the users, which would alter their decision-making process and create a feeling of stress. This finding indicates that urgency cues are an essential indicator of a phishing message. If it is true that an urgency cue is also a deception indicator, then it also stands to reason that paying attention to it would lessen the likelihood of the user responding to a

phishing e-mail, rather than increase the likelihood of responding to it, which would further suggest a contradiction on the previous findings.

The contradiction can be explained by further findings of Wang et al. (2012, 350), who also found, that when users are more knowledgeable of email-based scams, they would be more likely to pay attention to deception indicators, and less likely to respond to phishing emails. Thus, it seems that the initial findings shown by Wang et al. as well as Vishwanath et al. are put in a significantly different position when the user in question is knowledgeable of email-based scams. In a manner of speaking this means that some of the factors that have been found to increase the likelihood of the user responding to a phishing email have the opposite effect on the users that are knowledgeable of the scams.

3.1.3 Contextual indicators

The previously mentioned technical and social indicators alone are not necessarily a sufficient tool for analyzing phishing attacks. Literary analysis shows that previous research on phishing and social engineering has been, to this day, highly divided. It is still lacking a common consensus, a widely accepted conceptualization. Tetri and Vuorinen (2013, 1014-1018) argue that social engineering, in previous research, is often presented as an act that mainly consists of an attacker manipulating a victim, and that it does not take into consideration matters such as organizational setting, information security policy and user education, among other things. Tetri and Vuorinen further argue that the field of social engineering research demands a multidimensional framework that takes context into consideration.

The importance of context within the domain of phishing becomes evident when considering the act of spear phishing. In spear phishing, the attacker uses personalized information concerning the victim or their related organizational setting to get the victim to feel at ease with divulging information to the attacker.

As referenced earlier in section 2.4.12, improved contextual awareness has been shown to increase the likelihood of social engineers gaining the trust of the victims (Jagatic et. al., 2005, 1). It has thus been shown that context matters within the domain of phishing attacks and social engineering.

The focus of this thesis concerning context will be on the contextual indicators pertaining specifically to the victim and the victim's relationship with the attacker, which is most in line with the goals of this thesis. Context, even when only relating to social engineering, is an immensely large topic to cover. This thesis will continue the approach that focuses on what the user sees, thinks, and does when encountering a phishing message.

To begin developing an understanding of contextual phishing indicators and the impact of context on recognizing phishing attacks, a sufficient base of knowledge concerning context needs to be established. Dourish (2004, 20) suggests that context is something that draws analytic attention to certain aspects of social settings. Schilit, Adams and Want (1994, 1) consider three important aspects of context to be where you are, who you are with and what resources are

nearby. Pascoe (1998, 6-7) defines context as the subset of physical and conceptual states of interest to a particular entity.

Dey (2001, 2) suggests that some of the previous definitions for context such as the definitions by Schilit et al. and Pascoe are too specific and do not take all the relevant factors of the situation into consideration, at least within the environment of computer software development.

Abowd, Dey, Brown, Davies, Smith and Steggles (1999, 3-4) define context within the domain of computer science and application development as "any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves".

The notion of contextual understanding in phishing communications can be directly related to Goffman's frame analysis theory. As previously mentioned, the keys discussed by Goffman, in the context of this thesis, are what we call indicators. They are the variables that transform an activity into something that it is not. The transformation process itself is called keying. In the case of social engineering, this process is called fabrication, the difference between the two being the level of involvement of the user. In the case of keying, all parties are aware of the on-going transformation, whereas in the process of fabrication, the user should not be aware of the fabrication, or at least that is the goal of a social engineering attack.

There are some research articles that have directly discussed context within the domain of phishing attacks. Jagatic et al. (2005, 1) discussed the notion of so-called context aware phishing, in which attackers would gain the trust of victims by obtaining and subsequently referencing information about their bidding history or shopping preferences in a setting such as eBay. Another way to call context aware phishing is spear phishing. This take on context is relevant to understanding phishing, especially when trying to understand what makes phishing attacks successful.

Greene, Steves, Theofanos and Kostick (2018, 7) found that when analyzing the decision-making processes of users that were targeted with phishing attacks, the individual work context of each user was a key factor in understanding why some users fell victim to the attacks and why some did not. The findings of Greene et al. suggest that the most important contributing factors to a user's decision-making process (i.e., the decision of whether to click a link or not) were alignment/misalignment with a user's work context, expectations, and external events. The authors found that due to the users' work context, some of the phishing emails that they received seemed plausible enough that they did not offer the messages any further deliberation. These findings further indicate the importance of context within phishing. Some users will find phishing messages to be believable due to them aligning with work events (for example, having recently ordered something and then receiving a message that contains "an invoice" for an item. Others will receive the same message and remember that they have not ordered anything and will immediately get suspicious of the message.

Mouton, Leenen and Venter (2016, 4-5) discuss 6 examples of compliance principles that are defined by them as the reasons why a target complies with the attacker's request. The principles indicate that contextual factors play an important role in why users comply with the requests of attackers. With a newly developed understanding of how context relates to phishing, these compliance principles can be used as a base for forming a hypothesis on what contextual indicators of phishing attacks could look like.

The principle of friendship or liking suggests that people are more willing to comply with requests from friends or people they like (Mouton et al., 2016, 5). The contextual factors within this principle relate to the social relationships that the user has with other people, specifically those that they like. Translating these factors into contextual indicators is not simple. On the other hand, when someone that is not known to the user sends a message with a request for information or some form of action, an indicator of phishing here could be spelled out as "an unknown person sends an unsolicited request for some type of action". However, if the attacker has spoofed their e-mail address or phone number, they could present themselves as someone known to the user and liked by the user, to gain access to the user's information. Thus, another contextual indicator that could be derived from this principle stands as "an acquaintance sends an unsolicited request for some type of action that is out of character for them"

The principle of commitment or consistency suggests that once committed to something, people are more willing to comply with requests that are consistent with this commitment (Mouton et al., 2016, 5). The key factor of this principle could potentially be work commitments and a consistency to perform work tasks according to the expectations that have been set for the user. Greene et al. (2018, 7) discovered that one research subject of a phishing research who fell victim to a simulated attack mentioned that they were always interested in acting on the messages that they received. This could relate to the work culture and different demands for a different position. For example, one work role could entail having to receive and quickly respond to many e-mails, while another work role, even within the same company, could very well demand less responses, and would entail receiving fewer e-mails altogether.

The principle of scarcity suggests that people are more willing to comply with requests that are scarce or decreasing in availability (Mouton et al., 2016, 5). In terms of how the principle of scarcity relates to user context, it is naturally largely dependable on the nature of the request. For example, if an attacker attempts to deceive the user by baiting them with the promise of a ticket to an event that all employees were to receive, but with the offer expiring after a set amount of time, some users might interpret this as an indicator of deception due to them knowing that all the employees at the workplace have already received tickets to that same event. Some users, on the other hand, may have received information that they would be receiving tickets to said event, but had not received theirs yet.

The principle of reciprocity suggests that people are more willing to comply with a request if the requester has treated them favourably in the past (Mouton et al., 2016, 5). Concerning reciprocity, user context might also be a factor that

determines what sort of behavior is deemed as favorable and what is just common human behavior.

The principle of social validation suggests that people are more willing to comply with a request if it is seen as the socially correct thing to do (Mouton et al., 2016, 5). The socially correct thing to do is likely to vary from user to user, depending on the communities and cultures that they part of. For example, some users might have lived or are currently part of a community that thrives on helping others. This can, in turn, lead to the user being more willing to comply with weird requests, seeing as they are only trying to be helpful, and this is the kind of setting that they are used to; people asking for help and people willingly helping others. Other users may be part of a culture that is stricter and perhaps enforces strict information security protocols that all employees should be aware of. In turn, this means that some users might find there to be indicators of deception when someone asks for help, other users would consider this to be normal behavior.

The principle of authority suggests that people comply more easily with requests received from people with more authority than they have (Mouton et al., 2016, 5). Factors concerning authority may also relate to context in an essential manner. To some users, it would be normal that their supervisor, manager or generally someone in a position hierarchically above theirs would ask for information or otherwise approach them via electronic communications. This kind of unsolicited approach would seem normal to those users and thus not an indicator of deception. To other users, this kind of approach would be unheard of, and they would be likely to question it. This is also a matter that concerns organization culture and the organization's information security procedures.

Hadnagy and Fincher (2015, 11) discuss an example of phishing, a very ordinary Nigerian 419 phish. They discuss the specifics of which factors of the message indicate that it was, in fact, a phishing message. These details relate directly to the context of the user. The authors mentioned that the receiver of the message does not know the sender or any of the parties that are mentioned to be relevant in the phishing message. Additionally, they also mentioned that it doesn't seem likely that the sender would know the person that the message is being sent to either. Hadnagy and Fincher also point out the spontaneity of the message, stating it to have come completely out of the blue. Based on the factor of spontaneity being an indicator of phishing, one potential contextual indicator could spell out as "Should the user generally expect to receive messages of this kind?".

In summary, contextual indicators relate to the notion of normality. The essential point to be made about context within the domain of social engineering is that to some users, a specific message in which the user is asked for information is normal, while to others, the same message would be highly abnormal. Good phishers use cheap tricks to confuse the user, while great phishers make the message seem completely normal in relation to the user's context and get them to act against their best interest without ever realizing the mistake they made.

3.2 Attack vectors and attack types

This section is dedicated to briefly explaining the different types of phishing attack vectors and attack typpes. According to Jakobsson and Myers (2007, 32), phishing can be perpetrated in many ways, and most attacks are hybrid variations that utilize a combination of different attack vectors and techniques to achieve success. This section will attempt to explain several variations of phishing techniques.

3.2.1 Email phishing

Hong (2012) states that the focus of phishing email is on utilizing social techniques rather than technical tricks to fool users. Jakobsson and Myers (2007, 32-33) refer to email being the most common attack vector for phishing. A typical attack scenario within email-based phishing is a user receiving a message that states a specific problem that the user needs to deal with. The message supposedly originates from a trusted source. The user is asked to act urgently. The message contains a link that is suggested to lead to the website of the faked source. The link ends up leading the user to a fake website that is used to collect their information.

Hadnagy and Fincher's (2015, 2) definition of phishing is the practice of sending e-mails that appear to be from reputable sources with the goal of influencing or gaining personal information. Although it seems like a stretch to claim that phishing only happens through e-mail, it does back up Jakobsson and Myers' previous take that email is the most common attack vector.

Figure 3 presents an example of e-mail being used as the attack vector. This is just one of multiple potential examples of e-mail phishing. The example presented in figure 3 is in line with the theory presented above. The message is presented as originating from a reputable source, in this case, a credit union. The message states a specific problem that the user needs to address. In this case, the approach of the message is a common case of the user's account access supposedly receiving limitations, and the user is asked to confirm their identity through a link in the message, that is then likely to lead to a malicious website, through which the user is asked to fill out personal information.

3.2.2 Vishing

Yeboah-Boateng and Amanor (2014, 297) refer to vishing as a form of attack where the attacker lures the receiver of the call to share personal information to the attacker through a phone call. The term is derived from combining "voice" and "phishing". Basic social engineering techniques are used in vishing in combination with techniques such as caller ID spoofing. Song, Kim and Gkelias (2014, 865) define vishing similarly. They refer to it as a variant of phishing in which phone calls are used to deceive victims, with the goal of getting them to disclose confidential information or transfer money. Vishing attacks make use of a

technique called caller ID spoofing to change the phone number that is shown on the phone screen, which further increases the legitimacy of the caller, in the eyes of the person receiving the call.

Hadnagy and Fincher (2015, 5-6) consider vishing to be a trick that scammers use to follow up phishing e-mails. The purpose of the call is to add credibility to a phishing e-mail by following it up with a call. They mention an example of vishing being used in this manner. In this case, an administrative assistant received an e-mail regarding an invoice. After receiving the e-mail, the assistant received a phone call concerning the same subject. The caller claimed to be a vice president within the company, and then asked the assistant to process the invoice. This led to the assistant opening the e-mail and clicking the link, which further led to a malware-containing file being downloaded to the assistant's computer and stealing information.

The mentioned example is a way in which vishing can be applied to use quite efficiently. It would be hard-pressed to see vishing work reliably as a standalone form of phishing. Its applicability seems to be reliant on combining it with other techniques. The e-mail phishing attack presented in figure 3 is a reasonable example in this case. As previously discussed, the message is presented as originating from a reputable source. The message states a problem that the user needs to solve. Through our previous analysis, we were able to find several indicators of this message being a phishing attack. Despite our knowledge, it seems reasonable to assume that there are users who would fall for the message on its own.

Now, imagine a common user that is not trained in information security practices receiving this message, and immediately afterwards receiving a phone call, much like the administrative assistant mentioned previously did. Our common user might not have fallen for this message on its own, but a phone call to follow up an e-mail immediately adds more credibility to the message. The number that the phone call is originating from can also be spoofed with the utilization of caller ID spoofing to make it seem like it is coming from a number that is owned by the organization mentioned in the e-mail. There is a multitude of ways in which the attacker can attempt to influence the user at this point. These influence techniques are discussed more in section 3.3.2 concerning social indicators.

3.2.3 SMS phishing

SMS phishing (or smishing) is a form of phishing. It uses SMS-messages to reach their target. Basic social engineering techniques are found in smishing attacks. Two main processes are suggested to be a part of this process, the first of which is the user receiving a message which is supposedly from a trusted source, such as the user's bank. The second part involves the user receiving a text message saying that their account has been frozen and that they need to do something to unlock it (Yeboah-Boateng and Amanor, 2014, 299). The purpose of the first message is to lure the user into a false sense of security, since the first message does not demand anything from the user. The second message is the actual phishing attempt, which contains a malicious link.

Sonowal (2020, 360) considers smishing attacks to have a few clear advantages. For one, smishing attacks do not require an internet connection. It is also noteworthy that the number of mobile phone users is high. Sonowal also notes that the response rate to SMS messages is higher than the response rate to emails, which may give even further an advantage to phishers.

Figure 5 shows multiple examples of SMS phishing. These messages use simple social engineering techniques to trick users. In addition to URL obfuscation, the messages also try to exploit feelings of curiosity by stating that the user has received a voice message or that their mobile service operator has issued a statement of some kind, and that the user needs to open a link to read or listen to the message. These techniques will receive further analysis in the section pertaining to social and technical indicators.

3.2.4 Phishing in video games

Hong (2012) states that phishing attacks can also occur in online video games. Blizzard Entertainment (2018) highlighted phishing attacks happening in the Massively Multiplayer Online Roleplaying Game "World of Warcraft", stating 3 primary ways phishing attacks can happen in relation to the game:

1. Phishing emails
2. In-game phishing
3. Phishing through social media

For the purposes of this thesis, this section will only cover in-game phishing. According to Blizzard, nearly all the in-game phishing attempts consist of someone impersonating a Game Master. Game Masters are Blizzard Entertainment employees that are a type of customer service representative for World of Warcraft (Wowwiki, n.d.). According to Blizzard, players can be contacted either through in-game private whispers or through the in-game mail system by someone that is impersonating a game master. The approach is usually based on either of the following two takes:

1. Reward
    a. This approach suggests that the user should visit a specific website because of the user having won a prize, usually an in-game cosmetic item.
2. Punishment
    a. This approach is usually based on the attacker claiming that the user has violated a policy or a rule, and that the user must visit a website and enter personal information to avoid the punishment.

Alabdan (2020, 2-3) also references phishing attacks happening through gaming-related platforms. Alabdan refers to a case in which an attacker initiated a phishing attack by leaving a comment on a Steam (a PC gaming platform) user's

profile. The comment advertised a "free skin giveaway" (a skin being a cosmetic game item). The comment also contained a link which directed the user to a fake website.

Despite the different platform in use for the phishing attack, the disciples of persuasion are like those found in other types of phishing attacks. The first, reward-based approach is based on taking advantage of feelings of greed, while the second, punishment-based approach utilizes feelings of fear.

3.2.5 Spear phishing

A variation of phishing that refers to a type of phishing that is "speared" at a specific target. Spear phishing can for example be done utilizing targeted emails with the purpose of getting employees to perform erroneous activities such as clicking malicious links, downloading malicious content, or giving up sensitive information. (Williams et al., 2018, 1). Spear phishing is more personalized than ordinary phishing. They are targeted attacks against specific individuals within a specific organization. (Parmar, 2012).

A variation of spear phishing is a type of attack called "Whaling". It is a form of spear phishing that is targeted against high-level targets such as CEOs (Hong, 2012). Pienta, Thatcher and Johnston (2018, 11) describe whaling similarly, suggesting it to be an attack that is directed "at senior executives or other high-profile targets within a business by using highly customized threat intelligence".

Spear phishing and whaling are seemingly extremely potential forms of attack. Consider, for example, the phishing message presented in figure 3. The original message itself is likely to just be a common spam phishing message that is sent to hundreds of thousands of users. But what if the message was sent to specific users based on meticulously collected intelligence. For example, the message could only be sent to users that are known to be customers of the fabricated author of the message. This could potentially increase the likelihood of the user responding to the phishing message. Considering this example further, the message indicates that some services have been blocked from the users. This spear phishing attack could be conducted at the same time as another cyberattack. This other cyberattack could be something that disrupts the normal services, leading the user to believe the message more, and thus react as persuaded in the message. There are countless more ways in which spear phishing can be successfully conducted.

3.2.6 Phishing through social media

Hong (2012) references phishing through social media. According to Hong, phishing attacks can also be conducted through different social networking sites. In addition to this, Hong also states that social media can be used to gather intelligence for improving the effectiveness of spear phishing attacks. Chaudhry, Chaudhry, and Rittenhouse (2016, 250) second this idea, considering social media

to be a potential platform for researching victims before spear phishing attacks. They refer to a study conducted by Jagatic, Johnson, Jakobsson and Menczer (2007, 3). The results of the study showed that 72% of users responded to a forged phishing email that appeared to be from friends.

Studies have shown that phishers have gained the trust of victims by improving their contextual awareness. This entails phishers gathering information concerning the users' bidding history and shopping preferences, their banking services, or their mothers' maiden names. Phishers can also gather information through social network sites such as Facebook, Linkedin and others (Jagatic et. al., 2005, 1).

Social media can certainly be an effective platform for performing phishing attacks, especially spear phishing attacks. Consider two examples of ordinary phishing attacks, presented previously in figures 3 and 5. On their own, a message from a credit union or a message asking to open a link that contains a voice message might not fool users. However, if a user were to receive a message from a friend on a social media site, indicating that they, too, received said message and that they performed the requested actions and that the messages were legitimate, this would be likely to increase the likelihood of the user falling for the messages. This relates to the previously mentioned persuasion principle of social proof, that suggests that when other people trust an author, so too, should they.

4 TOWARDS DEVELOPING A FRAMEWORK FOR ANALYZING THE INDICATORS OF PHISHING ATTACKS

Based on a developed understanding of phishing indicators, we will now be able to develop a framework for analyzing phishing communications from the user's point of view. The basic premise of this analysis framework is built around the three categories of attack indicators: social, technical, and contextual. Social and technical indicators are universal in that the indicators are seemingly similar despite the context of the attack. Contextual indicators, on the other hand, differ from attack to attack, relating heavily to the context of the user. To some users, a specific phishing communication may seem to be contextually believable due to the communication fitting, for example, their work context perfectly. To others, the illegitimacy of the message is apparent due to the communication not fitting into the surrounding context at all. It should be noted here that analyzing contextual indicators of phishing is difficult without having access to the user's views on the messaging and their personal context. The analysis presented further on in this thesis will serve as a test for finding out what the limits are for analyzing contextual indicators of phishing. Several inferences will be made based on assumptions of what the user's context could be, to showcase the potential of the analysis.

Figure 9 shows the basic groups of indicators. Social and technical indicators have been the focus of a wide variety of research previously. As such, their indicators are already grounded on previous research which has been highlighted within this thesis. Thus, the primary goal of this section is to develop a set of contextual indicators that can be used in analyzing recent phishing attacks, in combination with social and technical indicators. With the contextual indicators developed, an analysis tool that combines all three groups of indicators will be presented at the end of this section.

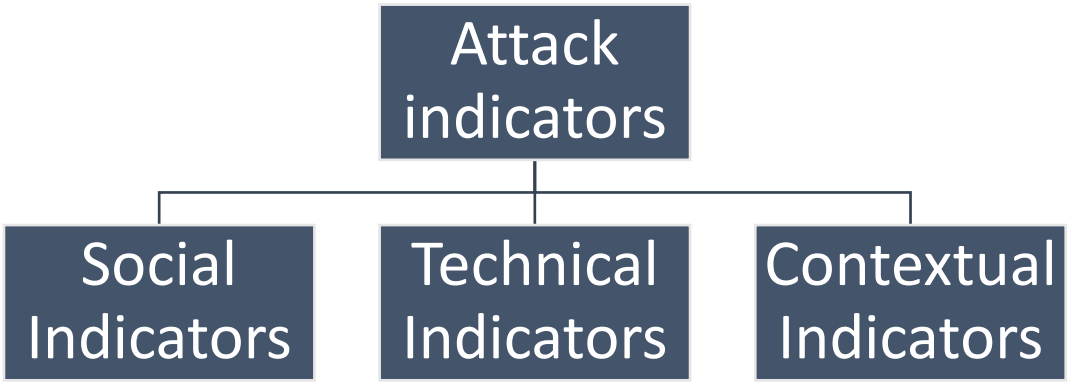


Figure 9: Attack Indicators

4.1 Developing a set of contextual indicators

As has been established in previous discussions, context can be defined as the information that defines the situation of an entity. This broad definition will serve as the basic building block of what contextual indicators of phishing attacks could look like. Simply put, when evaluating the legitimacy of a communication, users need to first ask themselves: "Does this communication seem believable in relation to my surrounding context?". This broad consideration, on its own, can already be a relevant contextual indicator that is just lacking in specifics. It covers a lot of ground but does not help in understanding the specific contextual indicators of phishing attacks.

As mentioned earlier, Schilit et al. (1994, 1) consider three important aspects of context to be where you are, who you are with and what resources are nearby. The keywords within this definition of context can be combined with knowledge on phishing and social engineering to start developing a set of contextual indicators.

Starting from the first consideration of what context is, "where you are". This question can be interpreted in different ways. For starters, it can mean the physical location of the user. However, it seems likely that the physical location of the user is often irrelevant in relation to social engineering. Thus, "where you are" should be interpreted differently. Social engineering attacks often seem to target businesses and organizations instead of private users. Based on this notion, within the context of social engineering, "where you are" can be considered to relate to the work role of the user, key questions being which company they are working for and what is their role in the company.

At least two ideas for contextual indicators can be derived from these questions. The first of these being, "Is it reasonable for the user to expect to receive messages of this kind in relation to their work role?". This indicator, while still being broad, does also go into more specifics. This indicator focuses on the individual's work role. For example, if a customer service representative of a large company were to receive a message in which the sender of the message is suggesting a profitable business opportunity for the company, it seems reasonable to question the message. The company might certainly have a single-place-of-contact policy in place, in which all communications go through the customer service. In this case, the message could potentially seem legitimate, at least in relation to this specific policy. However, it is also likely that the single-place-of-contact would not be the inbox of a specific customer service representative. It would be highly unlikely that the representative would receive a message of this kind in most circumstances imaginable.

The second suggested contextual indicator is: "Should the company that the user is working for commonly receive messages of this kind?". If the company is, say an accounting business, and a user working for the company were to receive an offer for taking part in a large-scale information system architecture development project, it does seem highly likely that the message is not a legitimate one. When evaluating incoming communications, it is essential to understand the surrounding work context: what company the user is working for and what their role is.

Drawing further from the definition of Schilit et al. (1994, 1) the next focus of analysis is on "who you are with". This statement can be connected to the social connections that the individual has. Previous research indicates that people are more likely to respond to phishing messages that appear to come from friends or from individuals that the user is otherwise familiar with. Leading from this notion, we can establish the idea of relating a contextual indicator to the notion of familiarity regarding the source of the message. In the case of the message sender being someone that the user is already familiar with on some level, a contextual indicator could be "Would this individual be likely to send a message of this kind to the user?".

Finalizing the analysis of the definition of context by Schilit et al. (1994, 1), "what resources are nearby" is the last topic of discussion. Nearby resources can relate to both the work context as well as the individual's personal life context. A typical phishing message (such as the one presented earlier in figure 3) often relates to some types of financial services, such as a credit union or banking services. It might be contextually normal for the user to receive messages from their bank but receiving them through SMS or e-mail instead of the bank's own messaging service might be out of ordinary. Equally out of ordinary would be for the user to receive a message relating to the user's own banking services from a different bank than which the user is a customer at. Thus, we can propose more contextual indicators of phishing: "Are the services presented in the message somehow related to the services that the user uses?", or "Is the received communication in line with the usual messaging of the service provider". Both serve as

indicators that demand contextual knowledge concerning the services that the user uses and how those services typically communicate with their customers.

As brought up earlier, Greene at al. (2018, 7) found that users would evaluate whether a message aligns with their work context, and specifically external events relating to the work context. The previously proposed contextual indicator "Is it reasonable for the user to expect to receive messages of this kind in relation to their work role" is a broad indicator that has its purpose, but a similar iteration of this can also be proposed based on the notion of alignment with external events. "Has the user previously done something that explains receiving this communication?". A reasonable example of this would be a recruitment process. If the user has applied for a job in a different workplace, they would expect to receive a call or a message from the company in question. Thus, to those users that have applied for a position, receiving a communication from said company would be completely normal and expected. Others, who have not applied for a different position, should generally not expect to receive a communication from a specific company, and if they do receive a communication, it would be smart of the user to properly evaluate the legitimacy of the communication before responding to it.

The definition of Abowd et al. (1999, 3-4) for context within the domain of computer science and application development, which was discussed earlier, can be used to further develop contextual indicators. The definition stands as: "Any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves". The essential part of the definition lies in the first sentence. "Any information", which is a very broad statement, "that can be used to characterize the situation of an entity", which limits the definition to information that can be related to a specific entity. The rest of the definition discusses what "entity" means within this context.

Context, within the domain of social engineering, is anything that explains the situation of a relevant party. This can be examined through some of the contextual indicators suggested earlier. Let us begin with two that relate to each other in that essentially, both consider the legitimacy of a received communication, either in relation to the role of the company or the role of the user, respectively.

- Is it reasonable for the user to expect to receive messages of this kind in relation to their work role?
- Should the company that the user is working for commonly receive messages of this kind?

Firstly, within these definitions, there are two entities that can be identified: the user and the company. The attempt here is to essentially explain what the situation of these entities is. Next, as per Abowd et al.'s definition, the goal of defining context is identifying "any information". The key, in both definitions, is the role of the entity. If it falls within the role of the entity to receive a specific

type of communications, then it is also reasonable to expect to receive those communications.

It is crucial to understand that even if the received communication falls under the umbrella of acceptable communications, it does not automatically mean that the communication is legitimate. Conversely, if the communication falls outside the commonly accepted norms in relation to the role of the entity, it does not automatically mean that the communication is not legitimate. This point is also relevant in relation to all indicators, not just the contextual indicators. Indicating something does not make it factual. It certainly points to a specific outcome, but a single indication does not make something an absolute truth. As such, the phishing indicators being developed here need to be treated as a combined analysis framework that is built to work as a tool that allows for the analysis of phishing communications with the goal of attaining a better understanding of the common features of phishing communications. This understanding should be used to further develop anti-phishing training materials aimed at the primary target of most phishing attacks: the common users that are not knowledgeable on information security practices.

4.2 Analysis framework

Firstly, regarding the development of an analysis framework for the purposes of this thesis, there is a challenge that needs to be considered, which was briefly mentioned earlier. Analyzing the surrounding context around phishing messages demands contextual knowledge. The issue with the materials that will be used is that for the most part, there is no contextual knowledge available. This means that the analysis of the contextual indicators of the phishing messages will be lacking. Despite this, a separate attempt of analysis based on the contextual indicators will be done. The goal of this separate analysis is to show how contextual indicators could function within phishing messages. To do this, educated guesses will be made regarding the context of the messages. Naturally, if contextual knowledge is available for a message, it will be used. Besides that, the gaps of knowledge will be filled with different scenarios that are deemed to fit the theme of the message. The goal is to make the context seem as believable as possibly so that it simulates the real world as closely as possible. The analysis of these made-up contexts will not provide factual knowledge regarding the statistics of the frequency of contextual indicators in phishing messages, which is why it is kept separate from the rest of the analysis.

Based on the previously presented discussions regarding context, phishing messages and context combined with phishing, a set of contextual indicators is proposed in table 2. These suggested contextual indicators are just a starting point. They are a very basic set of indicators that can still be expanded upon. Context is a broad concept that can have more detailed nuances, which would further separate and divide different contextual indicators into more specific sets of indicators.

Should the user reasonably not expect to receive communications of this kind in relation to their work role?	C1
Should the company that the user is working for commonly not receive communications of this kind?	C2
Are the services presented in the message not related to the services used by the user?	C3
Is the received communication not in line with the usual communication of the source?	C4
Has the user previously not done anything that explains receiving this communication?	C5

Table 2: Contextual indicators and their abbreviations

Moving on to another piece of the puzzle, social indicators (table 3). As previously established, there are multiple different ways of presenting different social indicators of phishing. Within this thesis, the chosen approach is deliberately broad. An essential factor to consider is the limitations of a common user. It is much easier to discuss basic emotions and social persuasion techniques such as fear, authority and empathy with a common user than discussing highly defined theories and abstract concepts.

Does the communication overly utilize feelings of fear or authority?	S1
Does the communication overly utilize feelings of curiosity?	S2
Does the communication overly utilize feelings of empathy?	S3
Does the communication overly utilize feelings of greed?	S4
Does the communication overly utilize urgency cues?	S5

Table 3: Social indicators and their abbreviations

Finally, a set of technical indicators that have been deemed to be relevant and recognizable to common users is presented in table 4. As outlined earlier, the focus of this thesis is on those indicators that are likely to be most relevant to the common users, i.e., the common users can be reasonably expected to recognize these indicators with little, or no training.

Does the communication contain a variety of grammatical errors or otherwise poor language?	T1
Does the communication utilize tricks of visual deception?	T2

Does the communication utilize URL obfuscation techniques?	T3
Is the website lacking a closed SSL padlock?	T4
Does the communication utilize spoofing techniques?	T5

Table 4: Technical indicators and their abbreviations

With the proposed indicators laid out, a basic tool for analyzing different phishing communications is proposed in table 5. Abbreviations are used for all the indicators to develop a form for gathering information that is easy to read and the findings are easily presentable.

Tech.	A1	A2	A3	A4
T1				
T2				
T3				
T4				
T5				
Soc.	A1	A2	A3	A4
S1				
S2				
S3				
S4				
S5				
Cont.	A1	A2	A3	A4
C1				
C2				
C3				
C4				
C5				

Table 5: Analysis form for analyzing phishing communications

The abbreviation 'A' stands for attack. The number after each A signifies which attack is being analyzed. This is a simple form that can be easily expanded based on the needs of the research. Each attack that will be analyzed will receive an abbreviation that has no other purpose than to separate it from the other attacks by specifically naming it, to make it easier for other parties to verify the findings later. The abbreviations do not have any other significance. Finally, the attack vector will also be specified with an abbreviation for each attack. "E" stands for e-mail, "S" stands for SMS and "W" stands for website. The attacks are separated based on their attack vector to discover if there are differences between the techniques primarily employed between the vectors.

The form will be used to document occurrences of different indicators in phishing communications. If a communication is found to contain a specific indicator, the correct cell will be marked with an "X". Each communication is thoroughly combed through to find all occurrences of an indicator. The same process is repeated for each attack that is chosen to be analyzed. The result is a collection of occurrences of different indicators in phishing attacks. The data can then be transformed from the analysis form into the number of occurrences and compared, for example, to the number of attacks analyzed to discover the frequency of different indicators in phishing attacks.

5 ANALYZING RECENT PHISHING ATTACKS

The phishing communications that were analyzed for the empirical data collection of this thesis were received from the national cyber security center of Finland, as well as directly from people who have received phishing messages, mostly in the form of e-mails. One screenshot was taken from a news article by the Finnish Broadcasting Company Yle. The messages were confirmed to be phishing messages based on them fitting the definitions and common indicators of phishing messages that were laid out during the earlier sections of this thesis. The language of the analyzed communications was primarily Finnish or English. One communication was in Russian, and one was in Swedish.

The sample size is 41 phishing communications, of which 13 are e-mail based, 12 are SMS or IM-based and 16 are phishing websites. Some of the indicators were found to not be applicable in the case of some attack vectors. In the case of indicators that were not applicable, they were not taken into consideration when calculating the percentages of indicator appearances in phishing communications. For example, technical indicator T4 is an indicator that relates specifically to phishing websites. Thus, T4 was ruled out of analysis when covering the rate of occurrence of E-mail and SMS or IM-based attacks.

As discussed earlier, the analysis of contextual indicators for the purposes of this thesis demands a user profile that is used to interpret how the contents of the phishing communications are seen. The user profile that is used here is that of the author of this thesis. The phishing communications in relation to the contextual indicators are analyzed from the author's personal point of view

5.1 E-mail attacks

In relation to the social indicators of e-mail attacks (Figure 10), the exploitation of feelings of greed was found to be the most prevalent of the indicators, being present in 92,31% of all e-mail-based attacks. In addition to feelings of greed, the utilization of fear and authority as well as urgency cues appeared quite

frequently, both having an occurrence rate of 53,85%. Exploiting the feelings of curiosity and empathy were found to have the smallest rate of occurrence, both standing at 23,08%.

The findings of this dataset are influenced by the nature of the analyzed attacks. The e-mail attacks analyzed for this thesis were, at least seemingly, for the most part, the kind of mass phishing / spam e-mails that most internet users are highly familiar with. They very likely lacked personalization and targeting, and thus were likely not spear phishing attacks, though this cannot be verified. In targeted spear phishing attacks, the occurrence of the exploitation of fear or authority as well as urgency cues might be higher. The utilization of greed might be slightly lower or unchanged. This is, however, only a speculation of what could be. As has been established, the contents of a phishing message may vary highly, based on the nature of the attack. User context may also have a significant impact on what the contents of the attack are, at least in the case of spear phishing attacks.

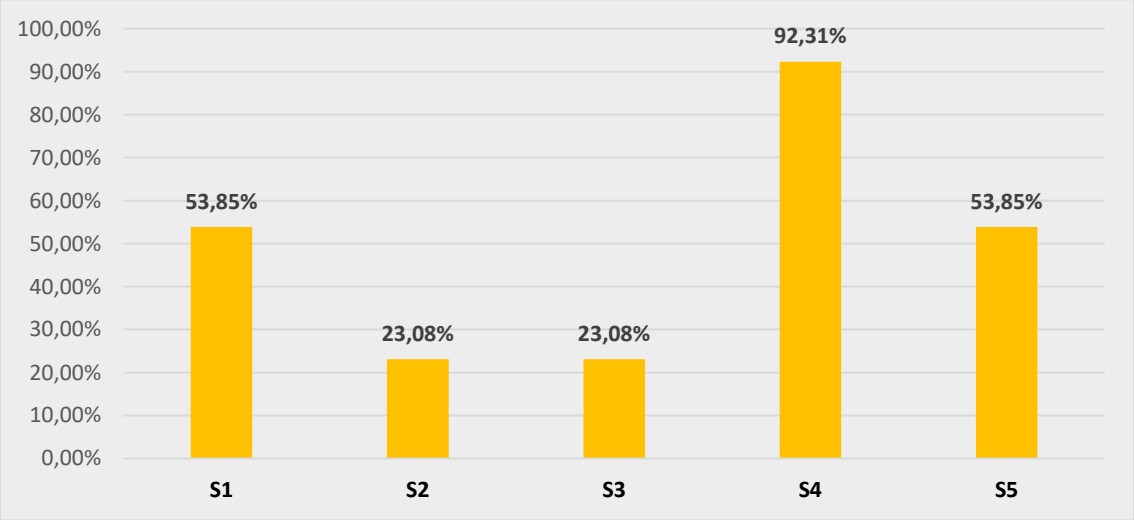


Figure 10: Social indicators in e-mail attacks

Within the domain of technical indicators (Figure 11), it was found that grammatical errors or otherwise poor language were prevalent in most attacks. In addition, some forms of URL obfuscation were also found to be used in most of the attacks. In most cases, the URL addresses used were just unknown or large domain names or spoofed to look like a known domain. Tricks of visual deception were not heavily employed. The lack of visual deception techniques used can also relate to the semantics of the matters. Visual deception within the domain of written content also relates to both URL obfuscation techniques as well as spoofing techniques in that, based on the definitions developed earlier for visual deception, URL obfuscation and spoofing can also be considered forms of visual deception.

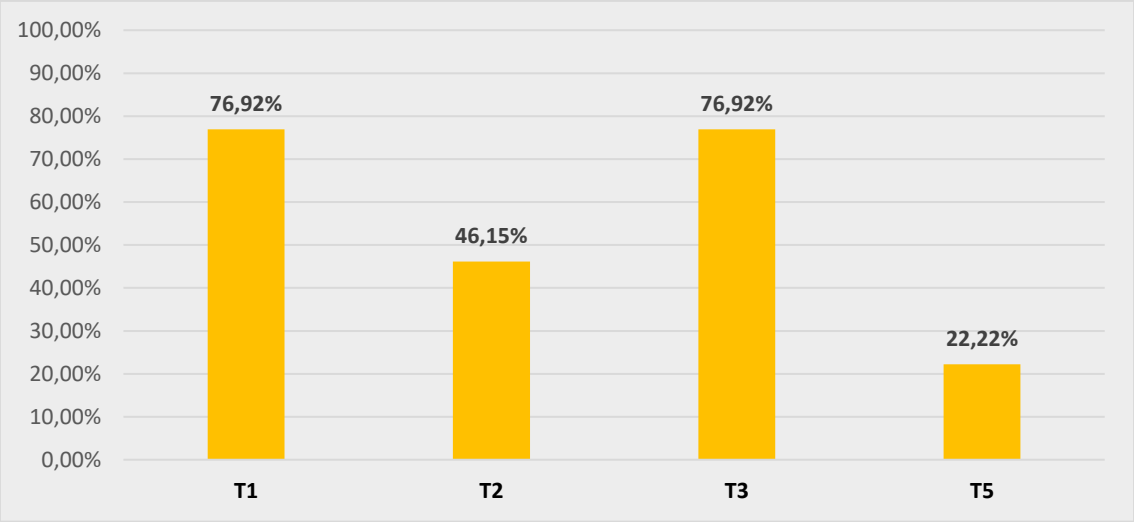


Figure 11: Technical indicators in e-mail attacks

The analysis of contextual indicators within the set of e-mail phishing attacks was done from the author's personal point of view. As these e-mail phishing attacks were seemingly the kind that were targeted at large masses instead of being spear phishing attacks, the messages can be analyzed by using the author as a profile. Because of the way the analysis of contextual indicators is conducted, the analysis of these contextual indicators does not provide accurate scientific findings that can be generalized into clear research results, but they do serve as a starting point for beginning to understand the importance of contextual indicators.

The findings showed that in the case of all the applicable contextual indicators, they were found to be meaningful indicators of phishing attacks. Despite only utilizing a single user profile to evaluate the messages, the results seem believable. It is certainly not a stretch to believe that the contextual indicators are highly prevalent indicators in all attacks. Nevertheless, these results still need further verification in more focused research where the profiles of the users are readily available.

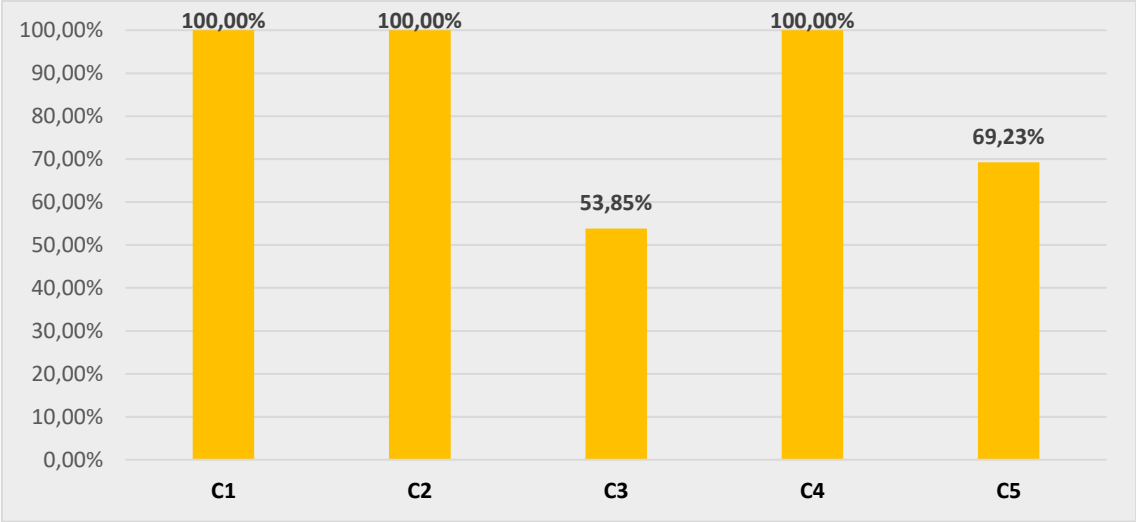


Figure 12: Contextual indicators in e-mail attacks

5.2 Phishing websites

An essential finding regarding the social indicators found on phishing websites (Figure 13) is that social persuasion techniques are not used often. The lack of social techniques can be explained by the websites being visually identical to the real websites, which is elaborated in the next paragraph. As they are visually identical to the real websites, any additional messages would make the websites seem less legitimate. It can be argued that the websites do use some forms of persuasion techniques, insomuch as the legitimate counterpart websites use them. For example, the websites of banks could be seen as utilizing feelings of authority to influence the user, simply based on the contents of the website being seemingly official in nature. Thus, a clear separation needs to be highlighted: when discussing the social indicators / persuasion techniques, the focus should be on how excessively they are used, and in what context they are used.

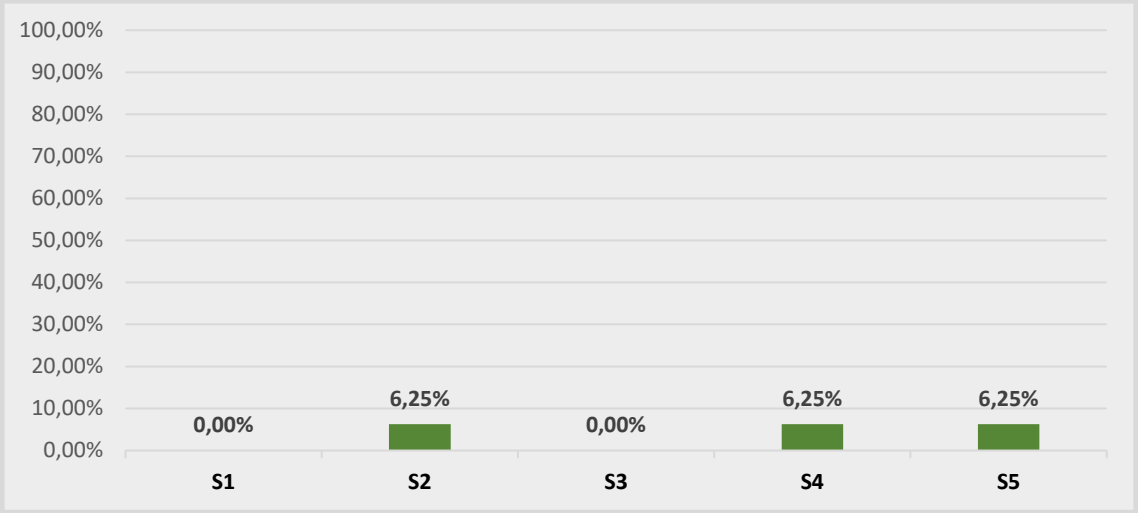


Figure 13: Social indicators on phishing websites

As mentioned earlier, concerning technical indicators on phishing sites (Figure 14), some forms of visual deception techniques are found in all the analyzed phishing websites. These sites are spoofed versions of actual legitimate websites of specific service providers, such as banks. A significant point regarding the visual deception techniques is that the spoofed websites are visually identical to the real sites in most cases. Even though the websites heavily utilize tricks of visual deception, this inference can only be made based on other indicators of phishing, i.e., the visual deception techniques are only identified as such due to having identified the website as a phishing site. Based on this, suggesting the utilization of visual deception tricks as a phishing indicator to the users can be detrimental, at least in the case of phishing websites. Similarly, most of the analyzed websites were found to use URL obfuscation techniques. The high occurrence of indicator T5 shows that all the analyzed websites were essentially fabrications of legitimate websites of legitimate service providers.

The low occurrence rate of indicator T1 is in line with the finding that most of the websites are simply fabrications of legitimate websites. As these fabrications are identical or nearly identical in terms of the contents of the website, it makes sense that they do not contain grammatical errors or otherwise poor language. Lastly, indicator T4 had an occurrence rate of 38,46%. This finding suggests that users should not consider a locked SSL padlock icon to be a sign of a legitimate, secure website.

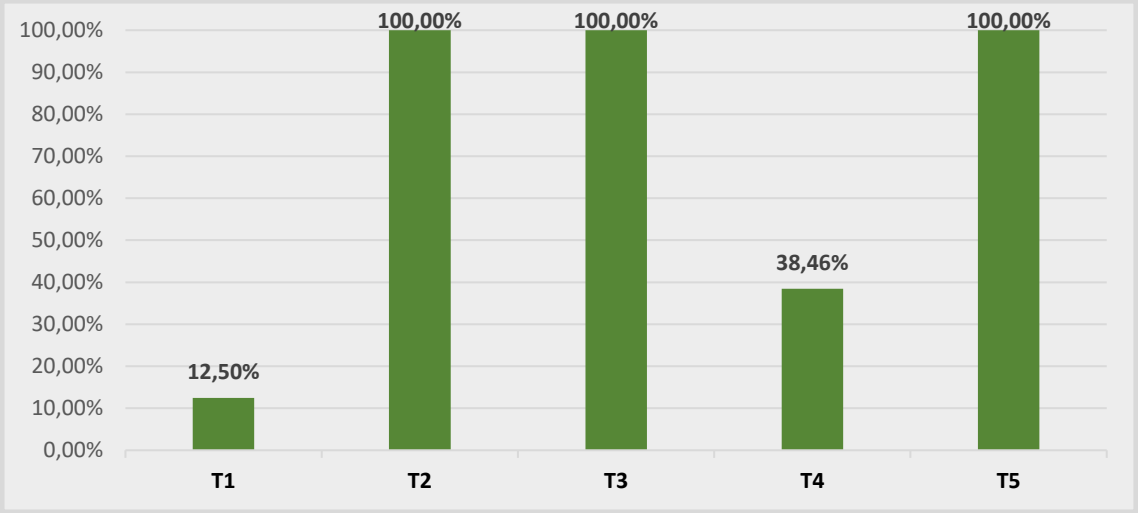


Figure 14: Technical indicators on phishing websites

A key takeaway concerning many phishing websites is that the clearest, and in some cases the only indication of the website being illegitimate is inconsistencies in the URL address of the website. Vigilantly paying attention on the address bar can thus be one of the best ways to recognize a phishing site.

Contextual indicators do not serve as a valid indicator of phishing in the case of most phishing sites, as shown in figure 15. Contextual indicators, in most cases, are not truly applicable when analyzing the contents of phishing websites. In most cases, the website is just one part of the attack, often not being an attack vector on its own. Indicator C4 was deemed as the only contextual indicator to have any sort of relevance when analyzing phishing websites. None of the other contextual indicators were found to be applicable for analysis.

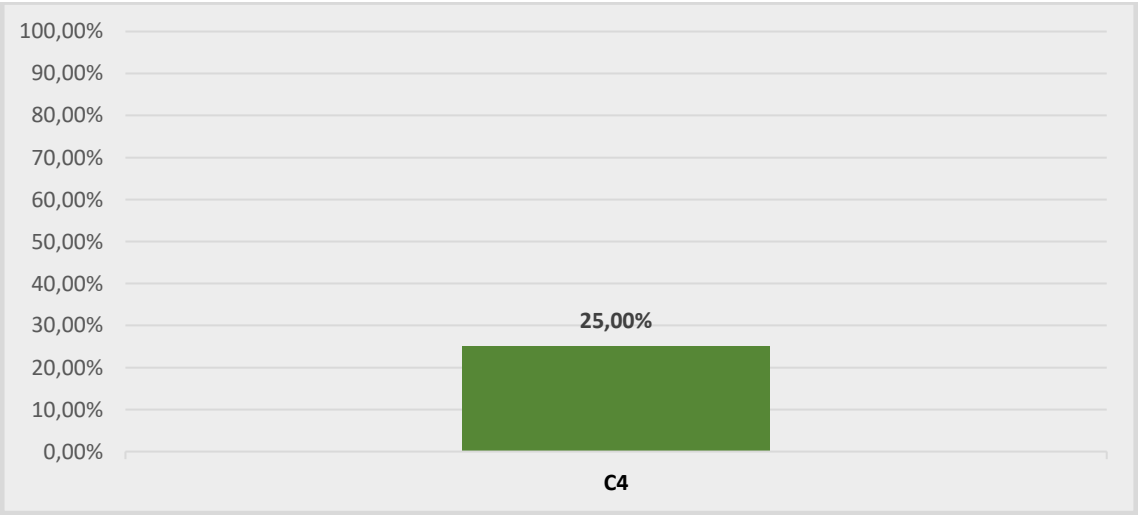


Figure 15: Contextual indicators on phishing websites

5.3 SMS / IM-attacks

Social indicators within SMS or IM-attacks (Figure 16) were found to appear in the attacks. Traditional SMS-messages are limited in the length of the messages, which in turn dictates the phishing techniques that can be utilized via SMS. Other IM communication platforms such as WhatsApp and Facebook Messenger allow for more personalized attacks that utilize different social persuasion techniques. Of the social indicators, indicator S2 had the highest rate of occurrence at 50%. This finding is in line with the idea that SMS phishing is limited by space constraints, which leads to the messages mostly only utilizing the curious nature of human beings with simple messages regarding packages being delivered to the user, followed up by a link for confirmation or something similar. Utilization of feelings of greed were discovered to be in 33,33% of the analyzed SMS / IM-attacks. Urgency cues had a very minimal rate of occurrence at 16,67%.

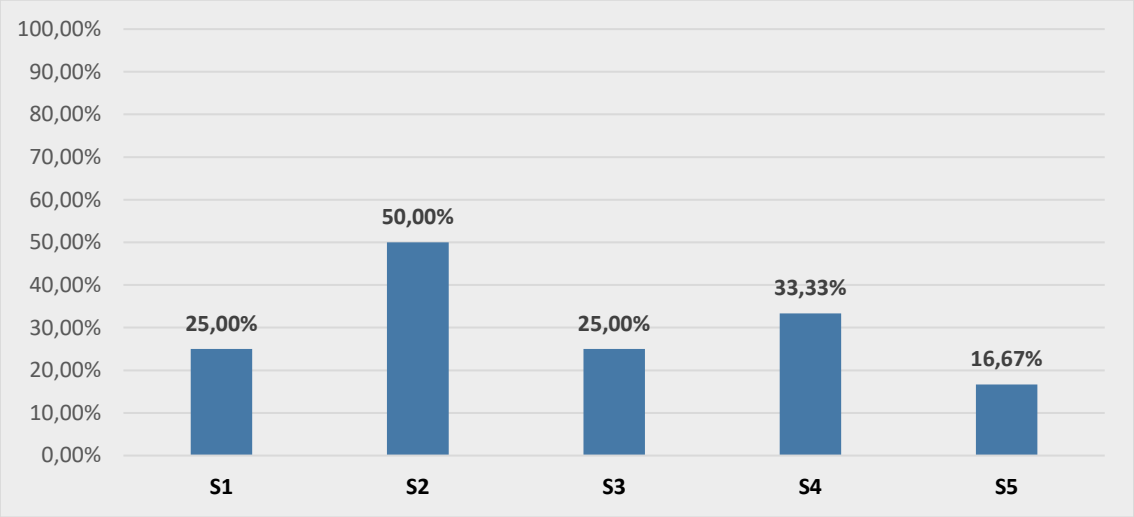


Figure 16: Social indicators in SMS / IM-attacks

Concerning the technical indicators within SMS / IM-attacks (Figure 17), all the analyzed attacks were found to have some forms of grammatical errors or otherwise poor language (T1). It is worth noting that while grammatical errors are, for the most part, a subject that is governed by clear rules of language, and does not, in theory, leave any room for debate about what is the correct way of spelling and writing, at least within the context of analyzing the language of phishing attacks. However, the language in some of the analyzed attacks only contained minor errors that some users might not even recognize as grammatical errors. With some of the messages being nearly perfectly written, in a grammatical sense, it stands to reason that those who perpetrate phishing attacks will improve their communication in the future to make the messages seem more legitimate. Nearly perfect fabrications of legitimate websites are one indicator for suggesting that phishing attacks are evolving in that direction. Essentially, this may mean that in the future, and perhaps even in the present, users should be advised

to not only pay attention on grammatical errors, but on other relevant factors as well.

It is important to note that none of the indicators presented in this thesis are, on their own, hard evidence for a communication being a phishing attack. The indicators simply serve as a collection of evidence that suggests a result to the question "Is this communication a phishing attack?". If a communication is found to contain multiple indicators of phishing, it is more and more likely that the communication is a phishing attack. However, a communication can just as likely be made to look so normal that it does not contain any clear indicators of phishing.

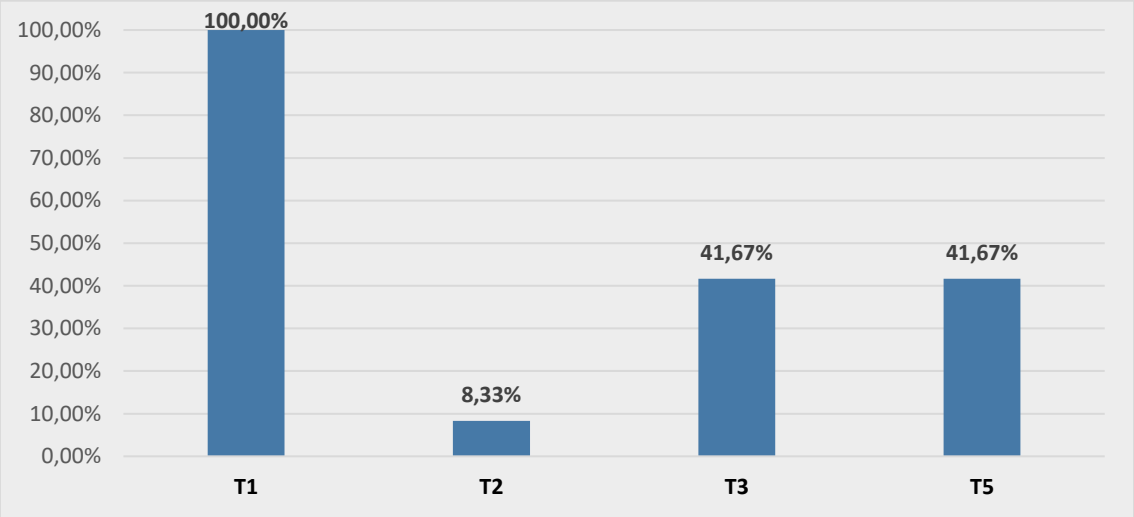


Figure 17: Technical indicators in SMS / IM-attacks

Contextual indicators were found to be highly prevalent within SMS / IM-attacks (Figure 18). In the case of indicator C4, out of the sample of 12 SMS / IM-attacks, 7 were found to contain indicator C4, while 5 of the attacks were not applicable based on the attacker not impersonating a legitimate source, and not being known to the user. With the usual communication of the source not being known, indicator C4 was deemed to be not applicable for analysis. Indicator C5 had a slightly lower rate of occurrence than the others. This was the result of the user having recently ordered some packages, leading to the received communication seeming slightly more legitimate, i.e., the user was expecting to receive confirmations from a postal service regarding a package. In a similar manner, indicator C3 had an occurrence rate of 81,82%. Occasionally, the services presented in a phishing message will fall along the lines of what kinds of services are used by the user, even if in most cases they do not.

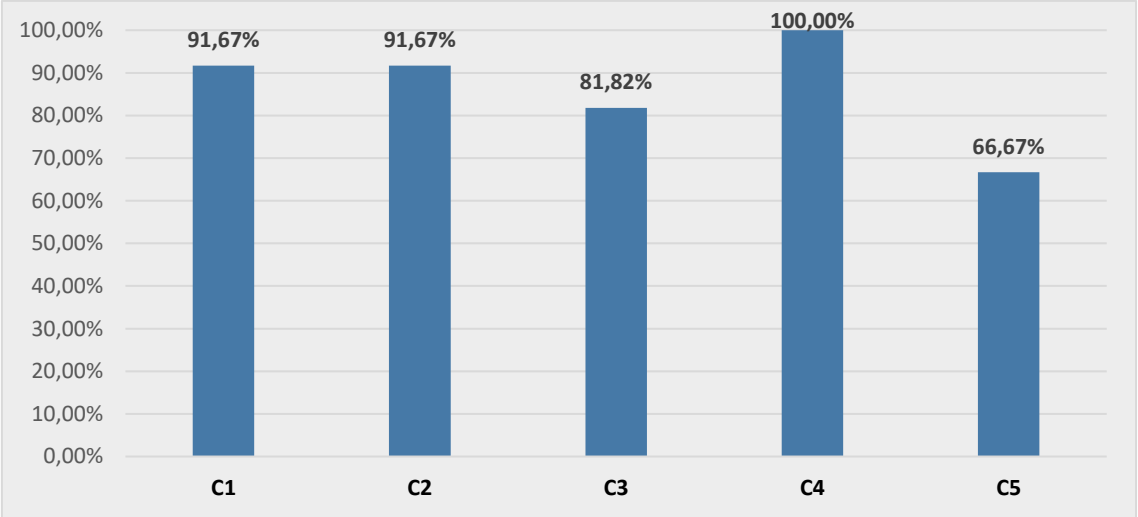


Figure 18: Contextual indicators in SMS / IM-attacks

5.4 Overall findings

None of the social indicators of phishing, while being theoretically applicable in all attacks, had a higher than 50% rate of occurrence in all the attacks combined (Figure 19). Social indicators were found to be more common within e-mail and SMS / IM-attacks, while there were next to no social indicators within phishing websites. This is explained by most of the phishing websites being fabrications of legitimate websites, resulting in those attacks not containing any social indicators. The utilization of greed was found to be the most prevalent indicator of phishing, appearing in 41,46% of the attacks overall.

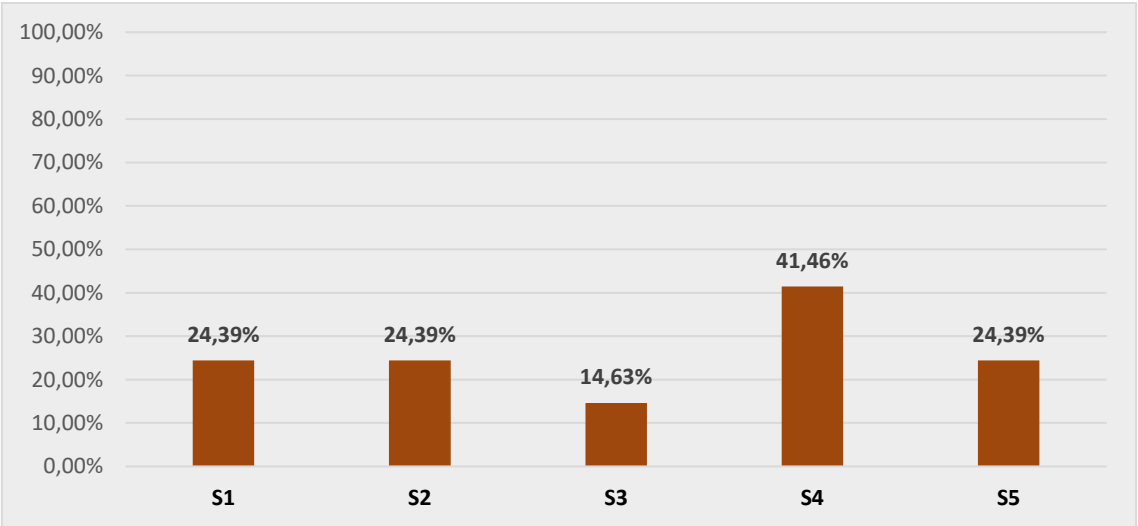


Figure 19: Social indicators in all attacks

The combined results of social indicators within e-mail and SMS / IM-attacks (Figure 20) paint a more accurate picture of how frequently users might expect to see social persuasion techniques being used within the attack vectors that they are commonly used in. Elements of greed (S4) were found to be the most commonly occurring indicator with a 64% rate of occurrence. Exploiting feelings of empathy (S3) had the fewest occurrences at a rate of 24%.

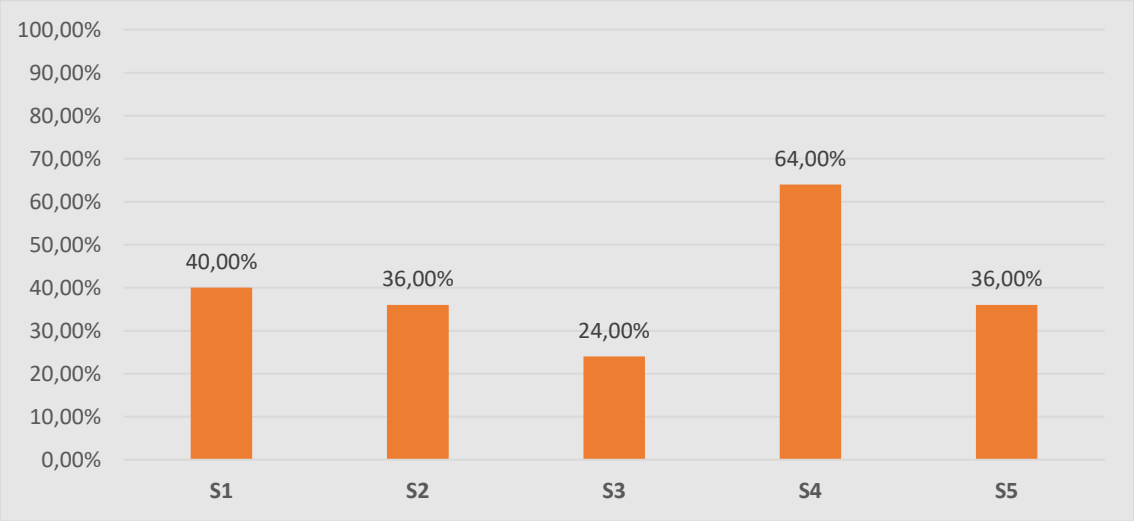


Figure 20: Social indicators in e-mail & SMS / IM-attacks combined

Most technical indicators were found to occur commonly in all the attack vectors combined (Figure 21). URL obfuscation techniques were found to be the most commonly occurring indicators. Websites lacking a closed padlock icon (T4) only had an occurrence rate of only 38,46%. As emphasized earlier, this finding strongly suggests that users need to be vary of websites even if they contain a closed SSL padlock.

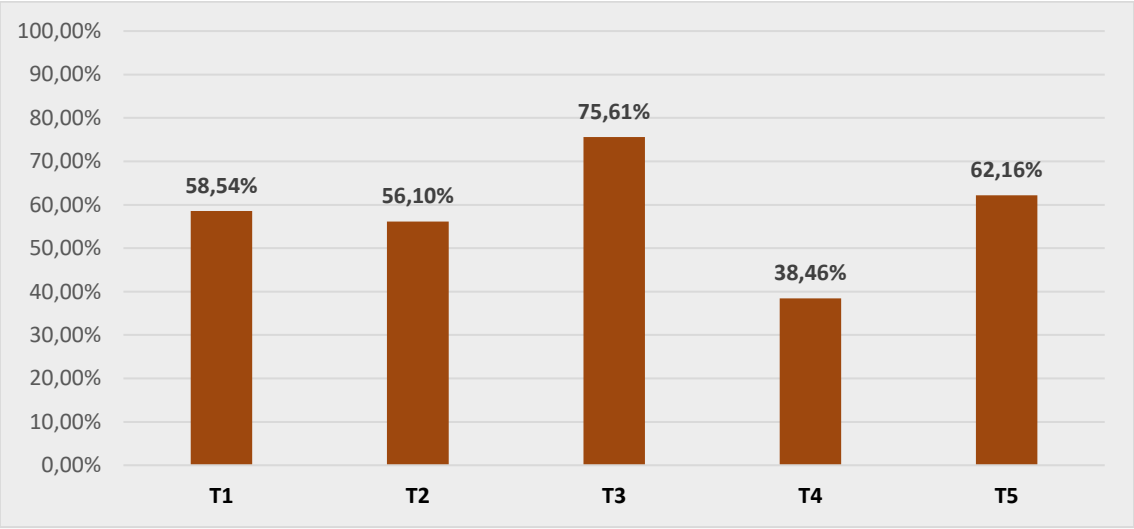


Figure 21: Technical indicators in all attacks

Finally, contextual indicators, when applicable, were found to have relatively high rates of occurrence while sampling a combination of all attacks (Figure 22). As has been highlighted previously, these findings are based on a single user profile, and as such the findings cannot be generalized into a larger population. Further research is necessary to validate the results and to find out the true significance of contextual indicators in phishing attacks.

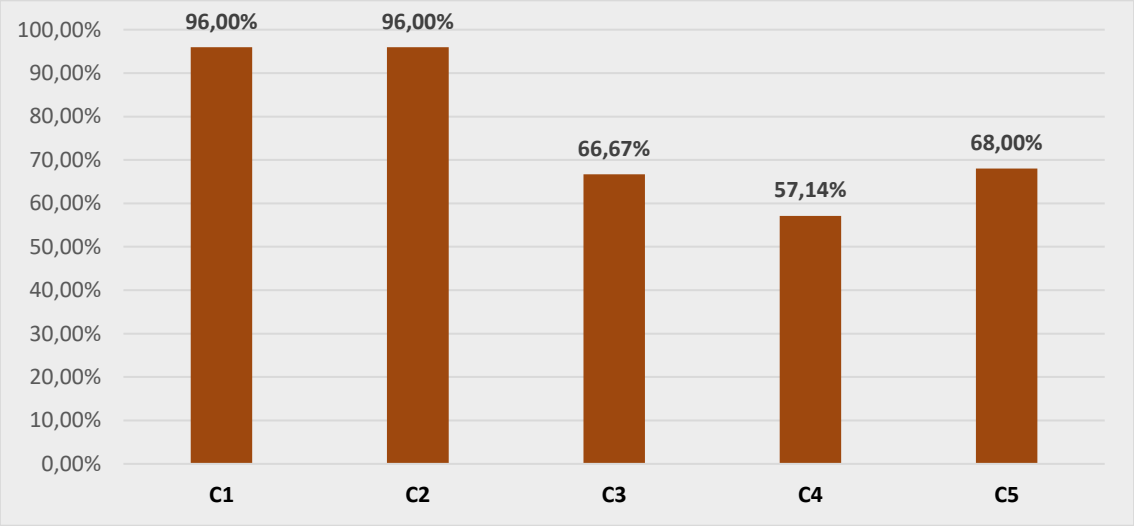


Figure 22: Contextual indicators in all attacks

6 CONCLUSION & DISCUSSION

The goal of this master's thesis was to develop an understanding of the features of phishing attacks from a common user's point of view. Analyzing previous literature on both social engineering as well as phishing specifically showed that there have been plenty of takes that discuss either the technical or social elements of phishing attacks. The approach of this thesis quickly developed into discovering if there is a significant connection between user context and phishing. In addition to matters related to user context, it was equally important to discover what the common social and technical indicators of phishing attacks are.

The research questions of this thesis have been answered, for the most part. Despite the limits of this research, it is safe to say that there are some forms of contextual indicators that can be recognized by the user as indicators of phishing. The common social and technical indicators of phishing have been determined, at least for the scope of this thesis. It is worth noting that, especially in the case of social indicators, there is still room for plenty of debate on what kinds of social influences constitute as persuasion techniques and how they are categorized. Within the scope of this thesis, a broad approach was chosen, the purpose of which was to determine which emotion or social theme was exploited. Some of the indicators could be split into smaller sets of indicators for more specific research results. However, since the approach of thesis was centered around the common user's point of view, it was deemed that a more generalized approach was best suited.

The more generalized and user-friendly approach was also relevant for the set of technical indicators. The set of indicators chosen was deemed to be the most user-friendly in the sense that the chosen indicators are more likely to be recognizable by common users as indicators of phishing than some other indicators might be.

There are some key takeaways from this research that need to be highlighted. Firstly, when comparing the occurrence of different indicators, contextual indicators seem to be the most common. As has been emphasized multiple times, the findings regarding contextual indicators are very preliminary and serve only as potential implications of how users might be able to recognize

phishing attacks. This finding suggests that users would be most likely to recognize a communication as a phishing attack by evaluating their personal context in relation to the received communication. This is, however, an oversimplified interpretation of the findings. If the user would only have access to one set of indicators, then this implication would be true. However, there is nothing disallowing the user from evaluating all the indicators available. It is the view of this author that determining whether certain communications are phishing attacks or not demands a comprehensive, multi-dimensional approach. User context is just one dimension that needs to be considered. Social and technical indicators serve an important role in recognizing phishing communications as well.

It needs to be stated that user context within phishing is not a simple subject to consider. The determined contextual indicators for this thesis are just one set of contextual indicators that can be utilized. There are certainly more concise contextual indicators that can be developed next to the ones proposed within this thesis, to properly cover different aspects related to context. For example, contextual indicators were not found to have a significant presence within phishing websites. This is explained with the fact that phishing websites are likely to be just one part of the attack instead of an attack vector. URL links in phishing communications that utilize e-mail or SMS / IM-messages as the attack vector lead to fabricated websites that are perfect or nearly perfect fabrications of legitimate websites. Essentially this means that none of the proposed contextual indicators that deal directly with the communication being analyzed and its relations to the user will carry any significance, as there is next to no difference to legitimate websites.

Other avenues for evaluating user context in relation to the websites could be proposed. For example, users might want to consider how they reached the website to determine its legitimacy. A potential contextual indicator here could be "Did the user reach the website in a different way than they have previously reached the website?". However, some users might be accustomed to finding a website by using search engines, which leaves them vulnerable to phishing attacks that exploit search engine optimization. In this case, the suggested contextual indicator would not work properly, as the users would have reached the website in the same way as they previously have, but they still reached a fabricated, illegitimate website.

Secondly, as already mentioned, most phishing websites seem to be perfect or nearly perfect fabrications of legitimate websites. This means that if users happen to reach a phishing website that is a fabrication, they will have a terribly hard time at recognizing it as a phishing site. Phishing websites were deemed to contain tricks of visual deception, but the users will not be able to recognize the visual deception as such unless they recognize the website as a phishing site through other means. Essentially this means that the findings concerning the appearance of visual deception techniques, within phishing sites, is mostly irrelevant, and should not be considered as a direction that user training needs to consider. It was also found that phishing sites did not contain many social indicators. The focus of anti-phishing training in relation to phishing websites needs to be on

other themes that are more reliable. Recognizing phishing websites as such seems to be largely reliant either on recognizing erroneous ways in how the site is reached or recognizing the website's URL address as falsified.

Thirdly, based on the findings of this thesis, it seems that the common phishing indicators found in communications are dependent on which attack vector is utilized. For example, it is quite often the case that SMS / IM-attacks do not utilize tricks of visual deception. These can, however, be found on phishing websites and e-mail attacks. Grammatical errors or otherwise poor language are often found in e-mail and SMS/ IM-based attacks but are nearly nonexistent on phishing websites. Social indicators are found on both e-mail attacks and SMS / IM-attacks, but with very different approaches. The e-mail format allows for more personalized content and does not have space constraints, whereas, especially in the case of SMS-attacks, the messages need to be short and thus cannot reliably deliver multiple forms of social persuasion techniques. Based on these findings, anti-phishing training should take into consideration the different approaches utilized in different attack vectors, and to train users in recognizing multiple different persuasion techniques and technical indicators. Anti-phishing training needs to function around a variety of attack vectors instead of just one or two vectors.

The findings within this thesis can be affected by the personal bias of the author. As the contextual indicators were developed for the purposes of this thesis, there might be an unconscious bias towards finding occurrences of said contextual indicators, thus supporting the theory that contextual indicators carry significance within recognizing phishing attacks. The findings regarding contextual indicators can also be impacted by the fact that evaluating them was based on a single user-profile, that of the author, which can lead to further inaccuracies. Due to this, it has been highlighted multiple times that the findings regarding contextual indicators need further research to be properly verified as significant factors in recognizing phishing attacks. A valid approach would be to either interview or survey multiple users that receive phishing messages and ask them to specifically consider their personal context in relation to the messages.

Besides the issue of personal bias, the problems of this research stem from context also being a rather difficult subject to research due to its subjective nature. Objective outside analysis of contextual factors is a tough undertaking due to different people potentially interpreting matters very differently from others. In relation to phishing, the user is the only one that can accurately understand their own context, and how the phishing communication relates to that context. Despite the difficult nature of context as a research subject, phishing researchers and information security practitioners should not shy away from it, and instead should look to further develop better experimental frameworks that seek to understand the big picture of phishing attacks, not just one part of them. Contextual indicators may well be one of the key parts of said frameworks. It is also possible that context is not a key element of those frameworks. At the very least, the experimental framework of phishing indicators presented in this thesis showed that there is a chance of contextual indicators being highly relevant, and that it is a

subject that deserves further research. No matter what the findings are in the future research, it is progress that helps understand phishing in a more comprehensive manner.

A noteworthy point that also needs to be considered regarding the sample size is that in the case of most attacks, evaluating the contents of one attack does not mean that it is just a single attack. Most often, the same attack is likely received by hundreds of thousands, perhaps even millions of users. Thus, the findings effectively reflect a very large number of attacks. With that said, this only applies to technical and social indicators. The findings regarding contextual indicators only reflect a single attack received by a single user due to context varying from user to user.

It seems likely that effective phishing communications are trying to "normalize" the communication by adapting to the context of the user, making it seem as normal as possible. If contextual indicators are indeed shown to be a significant phishing indicator, a direction of research that could also be pursued is developing e-mail and messaging filters that evaluate user context in relation to the communications received and determine if there are any factors that support the user receiving the message. If there are none or just a few, the message would then be flagged as a potential phishing message, thus taking as much decision-making away from the user, that has been established as the weak link of information security processes. This is certainly an interesting notion that comes with a wide variety of different issues, starting from this kind of advanced filter requiring plenty of personal information from the user. Handing out such information to private organizations is questionable, but at the same time, it is effectively already being done. E-mail spam filters also do already slightly evaluate context by flagging e-mails that originate from sources that the user does not often receive messages from.

Finally, it should be noted that the findings presented within this thesis are based on the material that was available for analysis at the time of writing. There might well be phishing attacks that are more sophisticated in terms of the techniques that they utilize. The analyzed phishing attacks are also believed to be non-targeted, mass phishing attacks that rely more on finding success through the quantity of attacks, rather than the quality of attacks. Targeted, personalized spear phishing attacks are likely to have more success and are also likely to utilize different kinds of persuasion techniques than the ones utilized within the sample of this thesis. Analyzing a set of spear phishing attacks would likely show very different research results and could also dictate the next steps of both phishing research and anti-phishing training. With that said, non-targeted mass phishing attacks remain a credible threat that demands just as much attention from information security practitioners as spear phishing attacks do.

REFERENCES

Abowd, G. D., Dey, A. K., Brown, P. J., Davies, N., Smith, M., & Steggles, P. (1999, September). Towards a better understanding of context and context-awareness. In International symposium on handheld and ubiquitous computing (pp. 304-307). Springer, Berlin, Heidelberg.

Alabdan, R. (2020). Phishing attacks survey: types, vectors, and technical approaches. Future Internet, 12(10), 168.

Alexander, J., Podgorecki, A. & Shields, R. (1996). *Social engineering*. Carleton University Press.

Ali, F. (2007). IP spoofing. The Internet Protocol Journal, 10(4), 1-9.

America's Credit Union. (n.d.). Contact Us. Retrieved 02/2022 from https://www.youracu.org/help-center/#tab2

Anti-Phishing Working Group (APWG). (2017). Global Phishing Survey: Trends and Domain Name Use in 2016. https://apwg.org/globalphishingsurvey/

Anti-Phishing Working Group (APWG). (2013). Global Phishing Survey: Trends and Domain Name Use in 2H2012.

https://docs.apwg.org//reports/APWG_GlobalPhishingSurvey_2H2012.pdf

Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N., & Arthi, S. (2020). Why is phishing still successful?. Computer Fraud & Security, 2020(9), 15-19.

Blizzard Entertainment. 2018. Spotlight on: Phishing. https://us.forums.blizzard.com/en/wow/t/spotlight-on-phishing/5492

Brody, R. G., Mulig, E., & Kimball, V. (2007). PHISHING, PHARMING AND IDENTITY THEFT. *Academy of Accounting & Financial Studies Journal,, 11*(3).

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. International Journal of Security and Its Applications, 10(1), 247-256.

Cialdini, R. B. (2006). Influence: the psychology of persuasion, revised edition. *New York: William Morrow*.

Credit Union National Association. (N.d.) Contact Us. Retrieved 03/2022 from https://www.cuna.org/about/contact-us.html

Deng, H., Wang, W., & Peng, C. (2018, October). Ceive: Combating caller id spoofing on 4g mobile phones via callee-only inference and verification. In Proceedings of the 24th Annual International Conference on Mobile Computing and Networking (pp. 369-384).

Dey, A. K. (2001). Understanding and using context. Personal and ubiquitous computing, 5(1), 4-7.

Dourish, P. (2004). What we talk about when we talk about context. Personal and ubiquitous computing, 8(1), 19-30.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems (pp. 581-590).

Ferreira, A., Coventry, L., & Lenzini, G. (2015, August). Principles of persuasion in social engineering and their use in phishing. In *International Conference on Human Aspects of Information Security, Privacy and Trust* (pp. 36-47). Springer, Cham.

Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007, November). A framework for detection and measurement of phishing attacks. In Proceedings of the 2007 ACM workshop on Recurring malcode (pp. 1-8).

Goertzen, M. J. (2017). Introduction to quantitative research and data. Library Technology Reports, 53(4), 12-18.

Goffman, E. (1986). Frame analysis: An essay on the organization of experience. Northeastern University Press edition.

Greene, K. K., Steves, M., Theofanos, M. F., & Kostick, J. (2018, February). User context: an explanatory variable in phishing susceptibility. In in Proc. 2018 Workshop Usable Security.

Grobler, M. M. (2010). Phishing for fortune. http://hdl.handle.net/10204/4553

Hadnagy, C: & Fincher, M. (2015). *Phishing dark waters: The offensive and defensive sides of malicious e-mails.* Wiley.

Hatfield, J. M. (2019). Virtuous human hacking: The ethics of social engineering in penetration-testing. Computers & Security, 83, 354-366.

Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74-81.

Howard, F., & Komili, O. (2010). Poisoned search results: How hackers have automated search engine poisoning attacks to distribute malware. Sophos Technical Papers, 1-15.

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. Heliyon, 7(3), e06522.

Irani, D., Webb, S., Giffin, J., & Pu, C. (2008, October). Evolutionary study of phishing. In 2008 eCrime Researchers Summit (pp. 1-10). IEEE.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100.

Jain, A.K., & Gupta, B. B. (2017). Phishing detection: analysis of visual similarity based approaches. *Security and Communication Networks, 2017.* https://doi.org/10.1155/2017/5421046

Jakobsson, M. (Ed.). (2016). *Understanding social engineering based scams*. New York: Springer.

Jakobsson, M. & Myers, S. (2007). Phishing and countermeasures: Understanding the increasing problem of electronic identity theft. Wiley-Interscience.

James, L. (2005). Phishing exposed. Elsevier Science & Technology Books.

Johnston, H. (1995). A methodology for frame analysis: From discourse to cognitive schemata. Social movements and culture, 4(2l), 7-246.

Jones, H. S., Towse, J. N., & Race, N. (2015). Susceptibility to email fraud: A review of psychological perspectives, data-collection methods, and ethical considerations. International Journal of Cyber Behavior, Psychology and Learning (IJCBPL), 5(3), 13-29.

Knopf, J. W. (2006). Doing a literature review. PS: Political Science & Politics, 39(1), 127-132.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology (TOIT), 10(2), 1-31.

Ledford, J. L. (2015). Search engine optimization bible (Vol. 584). John Wiley & Sons.

Ludl, C., McAllister, S., Kirda, E. & Kruegel, C. (2007). On the Effectiveness of Techniques to Detect Phishing Sites. Part of the collection: Detection of Intrusions and Malware, and Vulnerability Assessment, edited by Hämmerli, B. M. & Sommer, R. Lucerne : Springer.

Mouton, F., Malan, M. M., Kimppa, K. K., & Venter, H. S. (2015). Necessity for ethics in social engineering research. *Computers & Security*, 55, 114-127.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186-209.

National Cyber Security Centre. (2021). Fraudsters stealing banking credentials with fake My Kanta Pages and Suomi.fi messages. https://www.kyberturvallisuuskeskus.fi/en/fraudsters-stealing-banking-credentials-fake-my-kanta-pages-and-suomifi-messages

Parmar, B. (2012). Protecting against spear-phishing. Computer Fraud & Security, 2012(1), 8-11.

Pascoe, J. (1998, October). Adding generic contextual capabilities to wearable computers. In Digest of papers. second international symposium on wearable computers (cat. no. 98ex215) (pp. 92-99). IEEE.

Pienta, D., Thatcher, J. B., & Johnston, A. C. (2018, December). A taxonomy of phishing: Attack types spanning economic, temporal, breadth, and target boundaries. In Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy, San Francisco, CA, USA (Vol. 1, pp. 2216-2224).

Rader, M., & Rahman, S. (2015). Exploring historical and emerging phishing techniques and mitigating the associated security risks. *arXiv preprint arXiv:1512.00082*

San Martino, A. & Perramon, X. (2010). Phishing Secrets: History, Effects, Countermeasures. *Int. J. Netw. Secur., 11(3), 163-171.*

Schilit, B., Adams, N., & Want, R. (1994, December). Context-aware computing applications. In 1994 first workshop on mobile computing systems and applications (pp. 85-90). IEEE.

Singleton, R. & Straits, B. C. (2018). *Approaches to social research* (Sixth edition.). Oxford University Press.

Song, J., Kim, H., & Gkelias, A. (2014). iVisher: Real-Time Detection of Caller ID Spoofing. ETRI Journal, 36(5), 865-875.

Sonowal, G. (2020). Detecting Phishing SMS Based on Multiple Correlation Algorithms. SN Computer Science, 1(6), 1-9.

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. Behaviour & Information Technology, 32(10), 1014-1023.

Thomason, S. (2013). People–The Weak Link in Security. Global Journal of Computer Science and Technology.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576-586.

Vlajic, N., Chowdhury, M., & Litoiu, M. (2019). IP Spoofing in and out of the public cloud: from policy to practice. Computers, 8(4), 81.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. IEEE transactions on professional communication, 55(4), 345-362.

Williams, E., Hinds, J & Joinson, A. (2018). Exploring susceptibility to phishing in the workplace. https://doi.org/10.1016/j.ijhcs.2018.06.004

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security, 16(6),* 315-331.

Wowwiki. (n.d.). Game Master. https://wowwiki-archive.fandom.com/wiki/Game_Master

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?. Computers in Human Behavior, 84, 375-382.

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences, 5*(4), 297-307.