Tampereen yliopisto

Aleksi Rissa

FACTORS AFFECTING PHISHING SUSCEPTIBILITY

Bachelor thesis
Faculty of Information Technology and Communication Sciences
April 2023

ABSTRACT

Aleksi Rissa: Factors affecting phishing susceptibility
Bachelor Thesis
Tampereen yliopisto
Bachelor's programme in Computing and Electrical Engineering
April 2023

As electronic devices become more commonplace and web, mobile, and social media technologies continue to advance, cybersecurity is becoming a more crucial topic. Phishing is one typical attack vector that uses human weaknesses as opposed to system weaknesses. All cybersecurity systems rely on human judgment, which is frequently attributed as the weakest link.

With an emphasis on email phishing assaults in a business setting, this literature review investigates the numerous elements that affect the likelihood of a successful phishing attack. It was discovered that workplace characteristics, such as the degree of trust in the business and the level of technical understanding of the workers, as well as phishing attack tactics, such as the use of urgent language or threats, were found to impact vulnerability. Additionally, technical approaches, such as disguised links are used to further increase the likelihood of a successful phishing attack.

Studies that looked at the effectiveness of anti-phishing training in lowering susceptibility found that more regular and interactive training may be more beneficial. To successfully lower phishing susceptibility, the findings of this literature review emphasize the significance of a variety of preventative strategies, including both technical and human-centred approaches. To further understand how various factors affect phishing susceptibility and the best ways to mitigate it, more research is required.

Keywords: Phishing, Social engineering, Cyber security, Human vulnerabilities

TABLE OF CONTENTS

1. INTRODUCTION

Cybersecurity has become increasingly important, driven in large part by ever-evolving web, mobile, and social media technologies. The prevalence of electronic devices in everyday life and the constant increase in the amount of information available attribute to this. It is increasingly important for that information to be secure and while cyber-attacks are constantly evolving, so are the countermeasures through cybersecurity.

However, despite technological advances a there always remains a constant, the user. The user is a key part of system but are often attributed as the weakest link to it. Therefore, many attacks are made to focus the on the users rather than the systems themselves. One of the most common semantics-based attacks is phishing. It aims to exploit human vulnerabilities rather than system vulnerabilities. There are many types of phishing attacks, and the attack can be carried out in many ways. One of the most common mediums phishing attacks are carried out on is via email. This bachelor thesis is a literature review on the factors that affect phishing susceptibility. Almost all the studies examined in this thesis focus on a workplace environment with phishing experiments done via email. While human characteristics, for example age, ethnicity, or cultural background play an important role as factors in phishing susceptibility, it falls outside the scope of this thesis.

This literature study examines the different factors that influence the likelihood of a successful phishing attack via the means of reviewing numerous studies which have been made regarding those subjects. The second chapter briefly defines the concepts and processes that make up a phishing attack and outline any relevant additional information. The third chapter reviews previous studies on phishing susceptibility, initially by examining techniques used in phishing attacks and the effect they have on susceptibility. After this workplace factors that have an effect will be examined, finally moving on to examining the relation between anti-phishing training and susceptibility. The fourth chapter reviews findings from these studies to examine preventative methods that help reduce phishing susceptibility. The fifth chapter will outline the conclusions which will be drawn from examining the studies created on phishing susceptibility and explore the advantages of further study.

2. PHISHING AS AN ATTACK VECTOR

There are several different cybersecurity attack vectors, or ways by which an attacker can compromise the security of information systems and networks. These attack methods can include social engineering strategies that prey on people's vulnerabilities as well as methods that target technical flaws in hardware or software. These assaults have a range of goals, including as stealing confidential information, interfering with business operations, or dispersing dangerous software. Phishing is the use of semantic-based approaches or assaulting in a way that deceives the target into thinking they are doing something legitimate when they are doing something completely different.

2.1 Phishing

Social engineering is the art of manipulating people so that they give up confidential information or make the victim act in a different way from the usual. Phishing is a social engineering or semantics-based attack which attempts to solicit sensitive information from the victim or those around them. Due to the semantics-based nature of phishing attacks, they are also harder to detect which makes them an even larger risk in cybersecurity (Aleroud and Zhou, 2017). The issue with social engineering attacks in general is that there isn't a single way to eliminate them because they mostly involve the human element. (Aburrous et al., 2010).

An attack is classified as a phishing attack if spoofing procedure involves a website, and sensitive information from the entity is solicited (Aleroud and Zhou, 2017). In the case of an email phishing, the attacker and victim are in contact in some way. The attacker may impersonate anybody and may be carrying out the attack with as many targets as possible. In addition, phishing can be divided into subcategories depending on the attacks scope and target as presented in the Table 2.1. Email phishing, quantity matters more, as the hope is that someone, even if it a small percentage, respond to the attack in a way that is advantageous to the attacker.

Table 2.1. *Examples of different phishing attacks*

Type	Email phishing	Spear phishing	Whaling
Scope	Broad, targeted at as many people as possible	Narrow, targeted at certain individuals.	Very narrow, targeted at the" biggest fish"
Target	All company employees	Team leaders/organizers	CEO/CFO

Spear phishing attacks are targeted at certain individuals. The extreme case of this is Whaling, which targets the "biggest fish" in the corporation such as CEO, CFO… etc. In this case, even though the medium could be via email, the quality of the phishing attack matters a lot more (Frank et al., 2022).

2.2 Phases of a phishing attack

The phishing process can be defined into three step-by-step phases represented in Figure 2.1. The three parts it can be divided to are "Attack preparation, "Attack execution" and "Attack result exploitation".

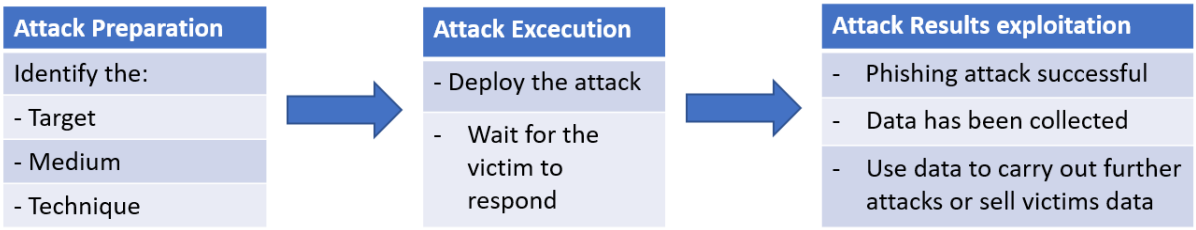

Figure 2.1. *Outline of the phases of a phishing attack.*

"Attack preparation" begins with the selection of the communication media used, though e-mail is by far the most common. Next is the selection of the target device or devices which make up the planned environment where the phishing attack will be made. After this, the attacker makes the choice of attack technique, for example website spoofing. Finally for the preparation attack material is prepared. In the context of an e-mail phishing attack, it would be the exact text used.

"Attack Execution" consists of attack material distribution, the gathering of target data, and the penetration of target resources. One or more victims may be exposed to the assault material. As soon as the targeted individuals react to the phishing attempt, target data

collecting starts. Additionally, attackers can compromise system resources to help with target data collection.

"Attack Results Exploitation" is the final part of a phishing attack. When the data has been collected from the targeted victims, their credentials may be used for various purposes, but very often to impersonate the victim to carry out further attacks. (Aleroud and Zhou, 2017)

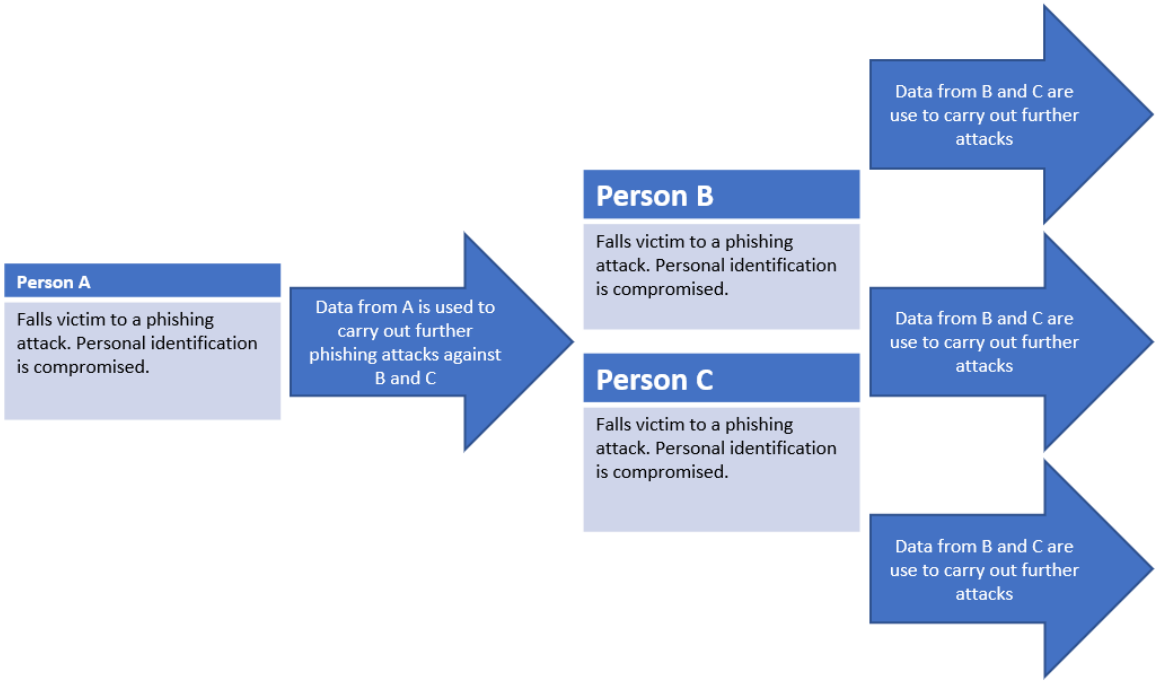

Figure 2.2. *How a successful phishing attack may lead to more successful phishing attacks.*

Figure 2.2 illustrates how when a single person falls victim to a phishing attack, it can lead to the compromise of entire networks or organizations. Attackers can use the victim's privileges to escalate their access and compromise other accounts and systems. Moreover, attackers can use the victim's credentials to launch additional phishing attacks against other individuals or organizations, posing as a trusted source. This can result in a cascading effect, where one successful phishing attack can lead to multiple others.

3. KEY FACTORS

Phishing is a manipulative technique aimed to fool the user to give up sensitive information. While there could be a magnitude of different factors that affect when a user falls victim to a phishing attack at play for each specific scenario, there are a few notable important factors found in the studies examined in this thesis. It all comes down to being able to spot the cues that would give a phishing attack away. Greater cognitive effort, more knowledge and experience help reduce the phishing susceptibility (Canfield et al., 2016). Some techniques used by phishing attacks make the users more likely to overlook key factors that would cue the user to the legitimacy of the email under normal circumstances. Workplace factors, training, and general knowledge of phishing attacks also play an important role in weather a user falls victim to a phishing attack.

3.1 Phishing techniques

The primary goal of the social engineering aspect in a phishing attack is to divert the user from making rational choices. Indicators of deceit and visceral triggers are the two key factors affecting a person's reaction to a phishing email (Wang et al., 2012). Certain triggers increase the risk of phishing susceptibility. Visceral cues, such as emphasizing the need for a response, raise risk of falling victim to a phishing attack, but general cues, such as grammatical errors and broken links, decrease the chance of a reply. The goal of visceral triggers is to provoke a variety of emotions in the victim, for example fear, greed, curiosity, or anger with the goal of making the victim act hastily without better judgment. Figure 3.1 is an example of a visceral trigger.

Figure 3.1. *Example of a visceral trigger, provoking the user.*

Social engineering techniques used to provoke a user response are for example authority, urgency, reciprocity, social proof, reward, loss, and scarcity (Williams et al., 2018). In an email phishing attack, authority could be used to convince the victim that the email is from an individual or organisation that represents an authority figure. Urgency can be used to convince the user that they have limited time to respond, thus provoking a hasty response. Reciprocity on the other hand implies that if the user responds to, they will gain some sort of

favour. Social proof aims to create the illusion that other people have already replied to the email to lure the victim to respond due to peer-pressure. Reward tries to imply that the user will gain some sort of reward or benefit. Loss on the other hand means the opposite where they will suffer some sort of loss by not responding. Scarcity is very similar to urgency but focuses on that the opportunity is limited in some way.

Technical approaches are also used on top of the social engineering aspect of a phishing to further enhance the effectiveness of the attack (Chiew et al., 2018). A key technical approach in phishing attacks is the Man-in-the-middle attack, where the attacker places themselves between the victim and a web-based application, essentially eavesdropping and collecting information. This makes the attack notably harder to detect as there should be no external indication to the victim that anything is out of the ordinary. URL obfuscation is another technique used to aid the efficacy of phishing attacks. The main goal of URL obfuscation is to either hide any suspicious parts of a phishing URL or make it mimic the real URL of website the victim might be familiar with. Examples of different methods of URL obfuscation are illustrated in Table 3.1.

Table 3.1. *Examples of URL obfuscation*

Original URL	Phishing URL	Changes
https://www.paypal.com/	https://www.paypals.com/	Character added
https://mail.google.com/	https://mail.goolge.com/	Character swapped
https://www.kela.fi/	https://www.kela.fi/	Character changed (L -> I)
https://www.reddit.com/	https://www.reddt.com/	Character Removed

To further aid phishers, there are a multitude of phishing kits available to generate faux websites, emails, or scripts to obtain user input. These do not require extensive programming knowledge to deploy, and technically by themselves do not gather personal information from victims, however they allow almost anyone regardless of their technical knowledge to deploy phishing attacks (Chiew et al., 2018). All of this can be done in conjunction with Man-in-the-middle attacks, further increasing the risk of successful undetected phishing attacks.

Spear phishing and Whaling are techniques that target specific individuals or individuals in an organization. The Effectiveness of such techniques can be high, because they use a special hand-crafted email mimicking an individual or organization the victim knows

(Chiew et al., 2018). A higher rate of success is achieved when the attacker communicates with the victim using the identity of the victim's friend.

3.2 Workplace factors

Social factors, workplace environment, physical contact all affect phishing susceptibility. It was found that a connection to a cybersecurity expert or help desk helps reduce the chance to fall victim to a phishing attack (Frank et al., 2022). Having a connection to a reliable source of information and a trusted person to ask decreases phishing susceptibility, whereas being part of a larger group of people increases it. Being higher up the corporate ladder also raises the risk as you are more likely to be targeted, i.e., spear phishing/whaling. Since the likelihood of having access to sensitive information increases the chance of being targeted by a phishing attack. The amount of time you have been in the working in the company increases the risk as users tend to get complacent. However, at the same time, an intern might not be given access to relevant cybersecurity training for resource management purposes (Frank et al., 2022). Finally, an increase of interactions between employees helped reduce the risk of phishing susceptibility. Being part of a smaller, more tightly knit group provides similar benefits as having access to a helpdesk or cybersecurity expert while also reducing the likelihood of a third party successfully impersonating a team member.

A high email workload also increased the susceptibility to a phishing attack. At the same time a very low frequency of phishing attacks increased phishing susceptibility. When faced with a high email workload and low frequency of attacks, the detection rate for phishing emails was near chance levels (Sarno et al., 2021).

4. PREVENTATION

Phishing attacks can be prevented through filters and blacklists, or more advanced credentialing systems, however many anti-phasing tools have false positives and are not always reliable (Nguyen et al., 2021). The weakest link in a security system is the often the user and biggest advantage attackers have in phishing attacks is the users' lack of education and awareness. It is imperative then that the user is given the best chances at noticing and not falling for phishing attacks. To this end it has been found that traditional security training is not always effective enough as a valid strategy (Aburrous et al., 2010). General mindfulness exercises had a greater effect on noticing phishing attempts than just focusing on examples of phishing attacks (Nguyen, Christopher, et al. 2021). In addition to this simulated phishing attacks with embedded training lowers the risk of a user becoming a victim of future phishing attacks (Jansson and Solms, 2013).

4.1 Automated methods

One specific subset of spam messages is phishing. To lure recipients to phishing websites is one of the key tactics used in phishing emails. It is possible to use an email filter to analyse emails and categorize them as legitimate or phishing emails. The primary method for doing this is to extract and analyse specific information from email headers and email body text Then, to classify the email, algorithms match those attributes to those in a legitimate email that are expected. (Almomani et al., 2013)

Blacklists can also be utilized to prevent possible phishing attacks. The client's browser automatically receives a list of potentially dangerous or suspicious websites. Websites can be blacklisted by search engines or users (Almomani et al., 2013). However, it has been found that users visit phishing websites despite the warnings (Nguyen et al., 2021). Whitelists could also be used, which only allow specific emails only. Unfortunately, whitelists tend to have a high false positive rate.

4.2 Training and awareness

Traditional training modules do not seem to be very helpful as a type of phishing awareness training when employees are already pressed for time. They may be excessively static and unresponsive in the context of the constantly evolving cyber security arena. (Williams et al., 2018). In addition to this, information overload can easily happen when employees are drowned in various other information such as health and safety notices. Constantly sharing the same notice about the dangers of phishing does not retain its effectiveness to keep

employees mindful on the subject. The addition of mindfulness training has been found to be effective in helping the user identify and avoid phishing attacks, however it is not fully effective. It can only reduce the amount of successful phishing attacks, not eliminate them completely (Jensen et al., 2017). However, relatively short anti-phishing training sessions can also be effective.

5. RESULTS

The findings of this literature study suggest that phishing susceptibility is influenced by several factors. The tactics utilized in phishing attempts, such as the use of urgent language or threats can enhance susceptibility and are one of the most crucial elements. For instance, research has shown that using urgent wording in an email's subject line might enhance the chances that it will be opened and that the assault would be successful. Threatening behaviour, such as threatening to stop a service or freeze an account, can also make people more vulnerable. In the end, the primary goal in a phishing attack is to divert the user from making rational choices, no matter how that result is achieved.

Workplace factors may also affect phishing susceptibility. According to studies, a person's workload, and access to trustworthy contacts in an organization affects how vulnerable they are, with those who have a higher level of trust being less likely to fall victim to phishing. The level of technical knowledge of the target population can also influence susceptibility, with fewer technically adept individuals being more vulnerable to phishing scams.

Some studies have also looked at the impact of anti-phishing training in lowering susceptibility. Anti-phishing training may be useful in raising knowledge and awareness of phishing assaults, but it may not always result in behaviour change. Training sessions that are more engaging and frequent may be more successful at lowering vulnerability in the long run.

The results of this literature study indicate the importance of a range of preventative tactics, including both technology and human-centred approaches, to successfully reduce phishing vulnerability. To do this, technical precautions like spam filters should be installed, and individuals must be educated about phishing schemes through training programs. It's critical to take workplace factors into account while developing preventative measures, as well as the strategies used in phishing attacks. More research is needed on the effectiveness of various preventative measures and the effects of various factors on phishing susceptibility to better understand how to counter these types of attacks.

6. REFRERENCES

Aburrous, Maher, et al. “Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies.” Cognitive Computation, vol. 2, no. 3, 2010, pp. 242–53, https://doi.org/10.1007/s12559-010-9042-7.

Aleroud, Ahmed, and Lina Zhou. “Phishing Environments, Techniques, and Countermeasures: A Survey.” Computers & Security, vol. 68, 2017, pp. 160–96, https://doi.org/10.1016/j.cose.2017.04.006.

Almomani, Ammar, et al. “A Survey of Phishing Email Filtering Techniques.” IEEE Communications Surveys and Tutorials, vol. 15, no. 4, 2013, pp. 2070–90, https://doi.org/10.1109/SURV.2013.030713.00020.

Canfield, Casey Inez, et al. “Quantifying Phishing Susceptibility for Detection and Behavior Decisions.” Human Factors, vol. 58, no. 8, 2016, pp. 1158–72, https://doi.org/10.1177/0018720816665025.

Chiew, Kang Leng, et al. “A Survey of Phishing Attacks: Their Types, Vectors and Technical Approaches.” Expert Systems with Applications, vol. 106, 2018, pp. 1–20, https://doi.org/10.1016/j.eswa.2018.03.050.

Frank, Muriel, et al. “Contextual Drivers of Employees’ Phishing Susceptibility: Insights from a Field Study.” Decision Support Systems, vol. 160, 2022, p. 113818–, https://doi.org/10.1016/j.dss.2022.113818.

Jansson, K., and R. von Solms. “Phishing for Phishing Awareness.” Behaviour & Information Technology, vol. 32, no. 6, 2013, pp. 584–93, https://doi.org/10.1080/0144929X.2011.632650.

Jensen, Matthew L., et al. “Training to Mitigate Phishing Attacks Using Mindfulness Techniques.” Journal of Management Information Systems, vol. 34, no. 2, 2017, pp. 597–626, https://doi.org/10.1080/07421222.2017.1334499.

Nguyen, Christopher, et al. “Learning Not to Take the Bait: a Longitudinal Examination of Digital Training Methods and Overlearning on Phishing Susceptibility.” European Journal of Information Systems, vol. ahead-of-print, no. ahead-of-print, 2021, pp. 1–25, https://doi.org/10.1080/0960085X.2021.1931494.

Sarno, Dawn M., and Mark B. Neider. “So Many Phish, So Little Time: Exploring Email Task Factors and Phishing Susceptibility.” Human Factors, 2021, pp. 18720821999174–18720821999174, https://doi.org/10.1177/0018720821999174.

Wang, Jingguo, et al. “Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email.” IEEE Transactions on Professional Communication, vol. 55, no. 4, 2012, pp. 345–62, https://doi.org/10.1109/TPC.2012.2208392.

Williams, Emma J., et al. “Exploring Susceptibility to Phishing in the Workplace.” International Journal of Human-Computer Studies, vol. 120, 2018, pp. 1–13, https://doi.org/10.1016/j.ijhcs.2018.06.004.