Topias Koski

INCREASE IN REMOTE WORK – EFFECTS ON PHISHING

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2021

TIIVISTELMÄ

Koski, Topias
Increase in remote work – effects on phishing
Jyväskylä: University of Jyväskylä, 2021, 53 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Etätyön määrä on kasvanut tasaisesti viimeisten vuosikymmenien aikana, mutta COVID-19:n ansiosta kasvu on suorastaan räjähtänyt. Samanaikaisesti tietojenkalasteluhyökkäysten määrä on kasvanut merkittävästi. Aiempi tutkimus esittää, että hyökkääjät ovat hyödyntäneet sekä etätyön lisääntymistä että COVID-19:ää. Etätyön lisääntyminen on innostanut ja aktivoinut hyökkääjiä. He ovat löytäneet uusia menetelmiä hyökkäysten toteuttamiselle. Tässä tutkimuksessa tarkastellaan etätyön lisääntymisen vaikutuksia tietojenkalasteluun. Tutkimuskysymys on seuraava: ”miten etätyön lisääntyminen on vaikuttanut tietojenkalasteluun?”. Kirjallisuuskatsaus paljastaa, että etätyössä tietojenkalastelijat ovat hyödyntäneet uusia teknologioita, yleistä hämmennystä, puutteita laitteiden turvallisuudessa ja puutteita IT-tuessa. Kohdistettujen tietojenkalasteluhyökkäysten määrä on kasvanut huomattavasti. Lisäksi haluttomuus hyödyntää uusia teknologioita altistaa työntekijöitä hyökkäyksille. Muutokset organisaatioiden sisäisissä toiminnoissa ja näistä johtuvat haavoittuvuudet ovat motivoineet hyökkääjiä uudistamaan käytettäviä menetelmiä. Osana tutkimusta järjestettiin kuusi puolistrukturoitua haastattelua. Tärkein löydös ja kontribuutio aiemmalle tutkimukselle on vastaajien kokema tiedonkulun heikkeneminen. Jokainen vastaaja mainitsi tämän potentiaalisena uhkana. Merkitystä korostaa, että tiedonkulku vaikuttaa olevan vahvasti yhteydessä muihin uhkiin. Uusien teknologioiden aiheuttama hämmennys ja haluttomuus niiden hyödyntämiseen ovat tekijöitä, jotka edesauttavat tiedonkulun heikkenemistä. Lisäksi kollegoiden välinen tuki voi heikentyä ja ensimmäiset toimet ja päätökset hyökkäyksen sattuessa voivat olla huonoja, koska tieto ei kulje kuten aiemmin. Tiedonkulun heikkeneminen altistaa tietämättömät työntekijät tietojenkalastelun vaaroille. Siksi niin organisaatioiden kuin yksilöiden tulisi miettiä uusia keinoja tiedonkulun parantamiseksi etätyöympäristössä. On suhteellisen aikaista määrittää, kuinka vallankumouksellinen etätyön aikakausi on tietojenkalastelun suhteen ja ovatko esille tuodut ongelmat pysyviä. Tämä tutkimus tuo kuitenkin esiin joitain uudistettuja turvallisuuteen liittyviä lähestymistapoja, jotka ovat huomionarvoisia tämänhetkisessä työskentely-ympäristössä.

Avainsanat: phishing, social engineering, etätyö

ABSTRACT

Koski, Topias
Increase in remote work – effects on phishing
Jyväskylä: University of Jyväskylä, 2021, 53 pp.
Information Systems Science, master's thesis
Supervisor: Siponen, Mikko

The amount of remote work has grown steadily during recent decades, but due to COVID-19 the growth has exploded. Simultaneously, the number of phishing attacks has significantly increased. Research suggests that attackers have utilized both the increase in remote work and the COVID-19 itself. The increase in remote work has inspired and activated attackers. They have found new methods for attacks. This research examines the effects on phishing caused by the increase in remote work. The research question is as follows: "how has the increase in remote work affected phishing?". Regarding remote work, literature reveals that phishers have utilized new technologies, general confusion, lack of security installation and lack of support. The number of spear phishing attacks has increased especially. In addition, the reluctance to take advantage of new technologies exposes employees to attacks. Changes in organizations' internal operations and consequent vulnerabilities have motivated attackers to reform their methods. As a part of the research, six semi-structured interviews were organized. The major finding and contribution to research is the decline in the flow of information experienced by respondents. This was mentioned by each respondent as a potential threat. The importance is emphasized by the fact that the flow of information appears to be strongly linked to other threats. The confusion caused by new technologies and the reluctance to take advantage of those technologies are factors that contribute to the decline in the flow of information. Furthermore, the support between colleagues might decrease and the first actions and decisions in case of an attack might be poor as the information does not flow as before. The decline in the flow of information exposes unaware employees to phishing threats. Therefore, organizations as well as individuals should consider new means to improve the flow of information in the remote work environment. It is relatively early to determine how revolutionary the era of remote work is regarding phishing and whether the raised issues are sustainable. However, this research highlights some reformed security-related approaches that deserve attention in the current work environment.

Keywords: phishing, social engineering, remote work, telecommuting

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

The amount of remote work has risen steadily for a long time (Ozimek, 2020). COVID-19, however, has forced employees to work remotely on an unprecedented scale. On the other hand, employers have been able to witness the largest remote work experiment to date. This might prove valuable for the future. It may be that working methods will no longer return to normal. Whether that happens or not, the 2020 footprints will provide the basis for future practices and ideologies (Leonardi, 2020). In any case, the threat of phishing has also risen steadily for a long time. Phishing is a form of social engineering that appears to be the most popular and arguably the easiest method to commit cybercrime (McAfee, 2018). Phishing refers to stealing sensitive information by exploiting human factors (Hong, 2012; Khonji, Iraqi & Jones, 2013). Phishing attacks result in exposures of sensitive data, financial frauds and identity thefts (Oest et al., 2020). COVID-19 has caused an increase in the growth of phishing attacks (NCSC & CISA, 2020; Ahmad, 2020). COVID-19 itself has been utilized in attacks but research also suggests that phishers seek to benefit from the increase in remote work. This research examines the role remote work has on the increase in phishing attacks. A threat to, so called, connected homes is not new, but the increase in remote work compounds home and business devices which results in new organizational threats and more connected devices in total (McAfee, 2021a). The major target of this research is to highlight the new threats posed by the situation as well as potentially intensified threats.

The research is conducted as a master's thesis on the field of information systems science. It compiles a literature review that supports and compares to the subsequent empirical research. The literature review provides an extensive overview of phishing, the concept and development of remote work, and the implications of these for each other. The empirical research, in turn, aims to add valuable information through data gathered from six respondents that have experienced the change from office work to remote work. Together, regarding the current topic, these approaches provide a comprehensive information package, indicative responses to the research question and important proposals for future research.

1.1 Research question

The research examines phishing in the renewed work environment. The research question is as follows:

> **How has the increase in remote work affected phishing?**

Answers for the question are sought through literature review and empirical research. The aim is to use one all-encompassing research question, which, however, includes multiple more detailed questions. The research focuses extensively on new threats that can now be identified as well as existing threats that have intensified. However, as the remote work has increased simultaneously with the threat of phishing, the effects on the working methods are also reviewed. Changed means of protection affect people's work and, on the other hand, non-compliance creates new internal threats. Through the research, in the literature review and in the empirical section, the aim is to constantly move forward in answering the research question.

1.2 Gathering the reference material

The reference material is mainly from recent years, and widely from 2020 since that year was revolutionary in terms of remote work. Therefore, not all references are as highly cited as would be desirable but, in any case, a wide variety of references have been reviewed and the most suitable ones have been selected for this research. Some older references are also included, partially because the developments of phishing and remote work are examined and also because it makes it possible to highlight changes in perspectives over the years. The literature has been selected mostly from a selection of high-standard information technology, information systems, information security and cyber security publications. Google Scholar is the major database used in gathering the references. ScienceDirect and Scopus are also used. The results of the research are somewhat indicative and longer-term experiences and statistics will be important for further research. The queries used in gathering the reference material included combinations of the words *phishing*, *social engineering*, *cyber security*, *remote work*, *telecommuting*, *telework*, *COVID-19* and *corona*.

1.3 Structure

The structure of the research is as follows. In chapter two, the main concepts are defined and phishing and remote work are reviewed separately. The last subchapter of chapter two focuses on the topic itself. Based on the limited research available, phishing on remote work environment is reviewed and the research question is answered based on literature. Then, in chapter three, the empirical research is presented. The goal, the used methods and the processes of preparation, data collection and data analysis are described. After that, in chapter four, the results of empirical research are examined. The last chapter consists of discussion, conclusions, contributions to research and practice, limitations, and proposals for future research. The conclusions and results of literature review and empirical research are discussed and comparisons are made. As desired, the results are mutually supportive, but even better, the results are also able to challenge each other. The primary recommendation is to read the entire research, as it provides a comprehensive information package regarding phishing in the remote work environment. Depending on the reader, if you want to move directly to the results, the secondary recommendation is to read chapters 2.3, 4 and 5.

2 LITERATURE REVIEW

This literature review defines the two main concepts of the research: phishing in chapter 2.1 and remote work in chapter 2.2. Chapter 2.3 examines phishing in the remote work environment. As Baumeister and Leary (1997) have stated, literature review serves as a bridge between the huge number of articles and a reader who usually does not have time to read all the articles. The literature review is conducted to create a concise information package for a reader. Presumably, this will support in understanding the purpose of the entire research.

The majority of the literature review was prepared before conducting the empirical research. However, in order to provide the most important background information as well as a good ability to read the entire research, the literature review was complemented after the empirical study was conducted.

2.1 Phishing

This chapter focuses on phishing. Subchapter 2.1.1 defines the key concepts related to phishing. 2.1.2 briefly describes the development of phishing to its current form. Subchapters 2.1.3 and 2.1.4 describe the methods of attacks and defence.

2.1.1 Phishing and its key concepts

In order to define the concept of *phishing*, it is reasonable to first define *social engineering* which is a close and similar concept to phishing. According to Engebretson (2013), it refers to exploiting a human weakness. The purpose is to get victim to reveal some confidential information (Engebretson, 2013). In the context of cyber security, or this research, Aldawood and Skinner (2018) define social engineering as follows:

> "In the context of cyber security, social engineering is the practice of taking advantage of human weaknesses through manipulation to accomplish a malicious goal." (Aldawood & Skinner, 2018)

In practice, social engineering may occur as a technique in which individuals are tricked to expose their credentials that, in turn, are used to access networks or accounts (Conteh & Schmick, 2016). In some contexts, the concept is also called human hacking (Conteh & Schmick, 2016; Hadnagy, 2010).

The line between phishing and social engineering is sometimes unclear, but both concepts have been explored and used extensively. However, as Conteh and Schmick (2016) state, social engineering is a category that includes other types of attacks in addition to phishing such as pretexting, baiting, quid pro quo, and tailgating. All these types aim to steal information or gain access to a restricted object or area (Conteh & Schmick, 2016). To highlight the scope of social engineering: shoulder surfing and dumpster diving are also stated (Luo, Brody, Seazzu & Burd, 2011) to be social engineering techniques. The first one refers to peeking over one's shoulder in order to obtain information. The latter one refers to looking over public trash cans in order to find some sensitive information that could be exploited directly or utilized in later attacks (Luo et al., 2011). The methods of various social engineering attacks differ but the attacks still have a shared malicious goal which is also the exact same in the case of phishing. In the research, phishing is broadly reviewed based on the following definitions:

> "Phishing is a kind of social-engineering attack in which criminals use spoofed email messages to trick people into sharing sensitive information or installing malware on their computers." (Hong, 2012)

> "Phishing is when an attacker tricks you into opening a malicious link or email attachment by masking them as something interesting." (F-Secure, 2021)

In other words, *phishers* seek to take advantage of the system vulnerabilities caused by human factor (Khonji, Iraqi & Jones, 2013). Phishers are the attackers who utilize social engineering techniques to simulate communications from trustworthy sources (Jensen, Dinger, Wright, & Thatcher, 2017). A typical way to attack is sending spoofed emails that ask for a link to be clicked and possibly direct user to fraudulent websites or ask user directly in the email field to provide information such as passwords or credit card details (Hong, 2012; Jakobsson & Myers, 2006; Jensen et al., 2017). Although email is the mostly discussed and mostly used (NCSC & CISA, 2020) platform among phishers, contrary to definitions of Hong and F-Secure, phishing may not always take place in the email environment. Phishing attacks may utilize phone calls, websites or SMS, for instance (Kang, Lee, Kang, Barolli & Park, 2014; NCSC & CISA, 2020). The basic principle is the same in these attacks as well. Therefore, the sweeping definition by McAfee might best serve the understanding of phishing:

> "Phishing is a cybercrime that aims to steal your sensitive information." (McAfee, 2021b)

The various platforms of phishing should be kept in mind when reading the research further. Although email-based attacks are widely used as examples, other platforms and techniques are also discussed.

2.1.2 The development of phishing

Jakobsson and Myers (2006) state that the first examples of phishing attacks occurred in the early 1990's on the America Online (AOL) network systems. Multiple hackers created fake accounts since the credit card validity tests were inadequate. It is stated that such attacks were not actual phishing. However, AOL improved its validity tests and soon, instead of creating fake accounts, the attackers began to steal other users' accounts by impersonating AOL authorities. With legitimate background stories and introducing themselves as AOL authorities, phishers managed to capture other users' passwords (Jakobsson & Myers, 2006). Rekouche (2011) reveals his own experiences from the beginning of phishing. The new AOL members were the primary targets of attackers since many of those had only a few minutes of Internet experience. At first, the fake account and the official-sounding name were created. The bait was then set in the form of a message asking for user's password or billing information. Messages were sent to users privately (Rekouche, 2011).

In principle, the phishing attacks were quite sophisticated in the early days since scam messages were written addressed to a specific group. At that time, however, the number of attacks was small. The success of the first attacks encouraged the attackers to expand their operations (Jakobsson & Myers, 2006). Gupta, Tewari, Jain and Agrawal (2017) present some milestones for the development of phishing. The term 'phishing' was first used in 1996 and declared by media in 1997. In 1999 the mass mailing was used to expand the attacks. In 2001 URLs had begun to be spoofed. In 2005 the term 'spear phishing' was first used. In 2007 more than 3 billion dollars was lost due to phishing (Gupta et al., 2017).

As the awareness of risks has improved, so has the quality of attacks. Although almost every internet user understands phishing at some level, they are still poor to, for example, differentiate legitimate websites from the malicious ones (Abbasi, Dobolyi, Vance & Zahedi, 2021).

The successful attacks have always inspired attackers to continue and expand (Jakobsson & Myers, 2006; Rekouche, 2011) and that is also true during COVID-19. During the ongoing pandemic, the number of phishing attacks has increased (NCSC & CISA, 2020; Ahmad, 2020). The amount of both the large-scale phishing attacks and spear phishing attacks has increased. These types and other, more detailed, methods of phishing are described in the following chapter.

2.1.3 Methods of attacks

In this subchapter, the process of phishing and its different classifications and types of attacks are examined. The process of phishing attack has five stages: attack planning, attack setup, attack execution, fraud, and post attack phases (Wetzel, 2005; Aleroud & Zhou, 2017). Aleroud and Zhou (2017) simplify activities into three main phases: preparation, execution and results exploitation. They also explain the subprocesses of each. In the first phase, attackers choose communication media, such as email, instant messenger or mobile app, in which the attack will be executed. In general, attackers also choose target devices such as smart phones or computers and attacking techniques such as website spoofing. Furthermore, attackers continue to prepare material for future attacks. In the second phase, firstly, the attackers distribute the prepared material to victim. Secondly, the target data collection starts when the victim responds to material as desired. Lastly, the attackers aim to facilitate user data collection using dishonest means such as adding client-side script to webpages. The third and last phase consists of target data usage and target resource exploitation. Usually the data from the victims, such as their credentials, is used for the identity theft (Aleroud & Zhou, 2017).

Phishing attacks focus on human weaknesses but, as Conteh and Schmick (2016) state, the attack techniques can be human or technical. In the first case, the attacker creates a relationship with a victim who is later exploited. The second case is more straightforward. The attacker steals information through, for instance, software, attachments and pop-up windows (Conteh & Schmick, 2016).

At its simplest, modern day phishing attacks can be classificated into two categories. Oest et al. (2020) state that those categories are (1) spear phishing attacks which emphasize the quality of attacks and (2) large-scale phishing attacks which emphasize the quantity of attacks.

According to Lin et al. (2019), to put it briefly, spear phishing is a more targeted version of phishing. In this case, a victim is often addressed by name. Persons with power or assets are often selected as targets because there is more to steal from them (Lin et al., 2019). Spear phishing attacks are proven to be significantly more successful than other kind of phishing attacks (Bullee, Montoya, Junger & Hartel, 2017; Steer, 2017). Spear phishing is made quite easy in today's society since social media channels offer a wide range of individual information (Parmar, 2012). One characteristic aspect of spear phishing is an opening phrase. As Bullee, Montoya, Junger and Hartel (2017) review, these messages often start with a phrase "dear [name]" where name is the actual name of the receiver. When they compare a message starting like that to a message with the opening phrase "dear employee", other content being exactly the same, it is proven that an email with a personalised opening phrase is significantly more dangerous than an email with a general opening phrase (Bullee, Montoya, Junger & Hartel, 2017).

On large-scale phishing attacks the number of targets is higher and the aim is to utilize volume rather than the quality of the message (Oest et al., 2020).

The large-scale phishing attacks have been utilized during the ongoing pandemic as the large-scale attacks containing pandemic-related claims have been alarmingly successful (Curran, 2020).

Although phishing has developed during recent years, email has remained as the most common platform for attacks (Jakobsson & Myers, 2006; NCSC & CISA, 2020). Email is somehow utilized in most attacks. Still, there are lots of differences in those attacks and their methods. Jakobsson and Myers (2006) divide phishing attacks into six types: (1) deceptive phishing, (2) malware-based phishing, (3) DNS-based phishing or "pharming", (4) content-injection phishing, (5) man-in-the-middle phishing, and (6) search engine phishing. Attacks often employ not just one but multiple technologies (Jakobsson & Myers, 2006).

In deceptive phishing, according to Jakobsson and Myers (2006), the most common vector is email. Typically, a phisher sends a deceptive email that presents some kind of problem but also a solution. The problem may concern, for example, victim's account information and it can be fixed by visiting a fraudulent website that gathers sensitive information (Jakobsson & Myers, 2006).

In malware-based phishing, some kind of malware (i.e., malicious software) such as keyloggers or trojans are involved, usually in order to infect victim's device (Jakobsson & Myers, 2006). Malwares may be spread when users open email attachments or download files from websites.

In DNS (Domain Name System) -based phishing, according to Jakobsson and Myers (2006), phishers utilize the domain name lookup processes. Hosts file poisoning is a major part of DNS-based phishing (Jakobsson & Myers, 2006).

In content-injection phishing, malicious content is injected into a legitimate website. The malicious content may redirect website users to other sites, install malwares on their devices or redirect data to phishing servers (Jakobsson & Myers, 2006).

In man-in-the-middle attacks phishers position themselves between users and websites (Jakobsson & Myers, 2006). Therefore, information that users hand over to these websites flows through phishers who can save the valuable information. As phishers are able to pass the information to the website and users may think that everything works properly, man-in-the-middle attacks are challenging to detect (Jakobsson & Myers, 2006).

In search engine phishing, phishers create websites that usually provide fake products, get the websites included in the search engine listings and aim to gather sensitive information from users through, for example, orders or sign-ups (Jakobsson & Myers, 2006).

Lastly, to describe the methods even more practically, a few more examples are given. Phishers might utilize loss or reward-based influence techniques (Williams & Polage, 2019). In other words, a scam message may indicate that the receivers are about to lose something, such as the access to the account, or about to get rewarded. To receive the reward, they need to click a spoofed link. Such attacks often create a sense of urgency, which affects the quality of decision-making (Conteh & Schmick, 2016). For example, a message might declare that an email address is about to get shut down and to avoid this, a link must be clicked or credentials must be given. Regarding the methods of attacks, there are also differences between genders. As Ragan (2013) and Conteh and Schmick (2016) state, against females, the common method is a message related to social networks. Against males, messages are often related to money, power and sex (Ragan, 2013; Conteh & Schmick, 2016). Highly targeted attacks, however, may utilize the psychological aspects of an individual (Ragan, 2013).

2.1.4 Methods of defense

When it comes to the question regarding the best countermeasure against phishing, there are two schools of thought. Phishing can generally be viewed from a psychological or technological perspective (Jakobsson & Myers, 2006) in which defense methods can also be divided into. Some consider user education the best countermeasure to phishing (Bailey, Mitchel & Jensen, 2008; Parmar, 2012; Aldawood & Skinner, 2018) whereas some prefer technical solutions (Jakobsson & Myers, 2006; Gorling, 2006).

According to Aldawood and Skinner (2018), user awareness can be increased through information security education, which decreases the number of successful cyber attacks. Gorling (2006) highlights that, when it comes to preventing attacks, it is not just about having knowledge or skills but rather utilizing those skills to promote security. Security solutions should be supportive rather than restrictive, and the security should never be a primary goal (Gorling, 2006). Presumably, ignoring all the, possibly suspicious, requests would be a solution against phishing. However, the consequential poor customer satisfaction would probably cost a company even more (Gorling, 2006).

In the combat against spear phishing, Parmar (2012) highlights the importance of constant education. Spear phishing is compared to pick-pocketing. Smarter users are less likely to become victims. However, since it only might take one individual to fall for fraudulent message, organizations must have a reasonable endpoint security strategy. One individual falling for scam should not compromise the entire network. A layered security strategy can add value by supporting the productivity, minimising compliance risks and producing a safety net for organizations (Parmar, 2012).

Jakobsson and Myers (2006) believe that education does not provide a long-term solution against phishing since phishers may also be educated and advised on how to carry out the attacks. Furthermore, they believe that constant education may lead people to avoid legitimate offers. If phishing is viewed from a psychological and technological perspective, they believe that technology provides better and more sustainable countermeasures (Jakobsson & Myers, 2006).

What kind of technical solutions can there be then? There are various different anti-phishing browser toolbars, proprietary toolbars and plugins (Li & Helenius, 2007; Abbasi et al., 2010; Abbasi et al., 2021). These solutions definitely add some value in the combat against phishing but, as Abbasi et al. (2021)

state, users often disregard warnings. This may be because warnings are not considered personal, addressed to the user (Abbasi et al., 2021; Chen, Zahedi & Abbasi, 2011). Zahedi, Abbasi and Chen (2015) offer a contextualization of research regarding fake-website threats and detection tools. In addition, they state that detector's accuracy, speed and response efficiency are the most important factors regarding users taking advantage of detectors when protecting themselves from malicious online actors and, therefore, those three factors should be invested (Zahedi, Abbasi & Chen, 2015). Fake-websites are a threat that could be responded with security toolbars, but a traditional email-based phishing might require different solutions.

Kirlappos and Sasse (2011) note that individuals are willing to take risks if there is little to lose. Furthermore, they criticize the state of security education since individuals often do not understand the details or significance of specific information or just do not want to invest in security enough (Kirlappos & Sasse, 2011). Indifference has far-reaching consequences as the successful attacks encourage attackers to engage in phishing (Rekouche, 2011; Jakobsson & Myers, 2006). Therefore, indifference contributes to the growth and spread of phishing. Instead of forcing individuals to read a large amount of information, security solutions could be adapted to their personal life and technology use (Kirlappos & Sasse, 2011).

Regarding the best countermeasure, there is not a clear consensus among researchers. Aldawood and Skinner (2018) state that technology alone does not solve human errors. Khonji, Iraqi and Jones (2013), in turn, question the significance of user education alone. They emphasize the importance of user education as a complementary part of technical solutions, although they mention the lack of research regarding this (Khonji, Iraqi & Jones, 2013).

Cyber security solution services provide instructions and guidelines to avoid phishing scams. The guideline by F-Secure (2021) is as follows:

1. Remember that you are your greatest vulnerability.
2. Understand that anyone can become a victim.
3. The many types of phishing often involve credible-looking sources.
4. Beware of urgency.
5. Trust your instinct.

Services such as F-Secure provide protection against known phishing websites (F-Secure, 2021) but, once again, technology alone might not be able to solve human errors. McAfee (2021b) encourages to check for the following signs when opening emails or text messages:

1. Is it poorly written?
2. Does the logo look right?
3. Does the URL match? (McAfee, 2021b)

However, spear phishing messages, especially, might be very well made. Recognizing those might require more developed knowledge or reassurance from colleagues. It might be reasonable to contact the sender or organization that emailed you, rather than opening suspicious links or attachments (McAfee, 2021b).

The combination of psychological and technical perspectives can be seen in today's tools, such as in Hoxhunt (2021), which is an email add-on that simulates phishing attacks. Those simulated attacks operate as disguised scam messages which are sent to employees. Basically, the employees should report those messages using the service. Based on their actions, they get positive or negative feedback. According to their website, Hoxhunt is an awareness training service but it also keeps users alert and supports the identifying of real threats (Hoxhunt, 2021).

2.2 Remote work

This chapter focuses on remote work. Subchapter 2.2.1 describes what remote work is and how it differs from other forms of work. The development of remote work is briefly reviewed in 2.2.2 Different types of remote work are discussed in 2.2.3 and typical remote work applications in 2.2.4.

2.2.1 Remote work and its key concepts

As Mokhtaryan (1991) states, defining the concept of remote work both broadly and restrictively enough is challenging. It is, however, defined as follows:

> "work done by an individual while at a different location than the person(s) directly supervising and/or paying for it" (Mokhtaryan, 1991).

Similarly, Olson (1983) states that remote work is organizational work carried out outside of the usual organizational space and time. Although remote work is the term mostly used in this research, *telecommuting* is a close concept in meaning and the differences between them are negligible. Nilles (1975) was the first to come up with the concept of telecommuting. It was stated that various telecommunications components enable employees to work near, but normally not at home (Nilles, 1975). Mokhtaryan (1991) suggests that a remote work can be treated as telecommuting if there are remote management and a reduction in commuting involved. Orlikowski and Barley (2001) have compiled the following definition. Telecommuting refers to utilizing technologies such as telecommunications and computers to work from somewhere else than one's declared office. Telecommuting is often talked about as a substitute for office work (Orlikowski & Barley, 2001). In general, the recent literature somewhat assumes that telecommuters work from home, but Orlikowski and Barley (2001) observe that home work is actually a separate concept since people may work remotely from airports or hotels, for example. *Teleworking* is another concept that often appears in literature. According to Mokhtaryan (1991), teleworking refers to the use of the telecommunications technology but does not necessarily qualify as remote work since teleworking might be performed at the conventional office. Telecommuting qualifies as both teleworking and remote work (Mokhtaryan, 1991).

2.2.2 The development of remote work

Research shows that the concepts of remote work and telecommuting have existed in the 1970s (Nilles, 1975) and self-employed professionals such as artists or writers have been working home even longer (Olson, 1983). However, it is relevant for the research to specifically define the development of technology-based remote work. According to Mokhtaryan's (1991) definition, the work done by the artist does not necessarily fall under the concept of remote work since there are possibly no persons supervising or paying. Sales work, in turn, is an example of remote work that has been performed for quite a long time and falls under the concept. On the other hand, for the purpose of this research, sales work is not a primary target of investigation. Instead, traditional office-based work that can be performed remotely due to advances in technology, and the development of such work is an important subject in this research.

Before corona, the amount of remote work has risen steadily (Ozimek, 2020), although its share of all work has been relatively small (Ozimek, 2019). Before COVID-19 was spread, remote work was supposed to grow due to improvements in internet, cloud and communications technology (Ozimek, 2019) but no one could have predicted the effect of COVID-19. It has affected remote work in an unprecedented way since people have been forced to work remotely. In the United States, of the people employed before COVID-19 spread, about half worked from home after the COVID-19 spread and one third of all employees had switched to working remotely (Brynjolfsson et al., 2020). In the United Kingdom 5% of employees worked mainly from home and less than 30% ever worked from home in 2019 (Office for National Statistics, 2020; Sarginson, 2020). 45% of UK workers expect permanent changes to flexible working after COVID-19 (O2 The Blue, 2020; Sarginson, 2020). Another US estimation suggests that 25 to 30% of the workers is going to work from home at least few days a week by the end of 2021 (Lister, 2020; Sarginson, 2020). Brynjolfsson et al. (2020) highlight a few observations. First, younger people have been more likely to switch to remote work. Second, there were no meaningful differences between responses in April and May in 2020. Third, in July employees began to slowly return to commuting (Brynjolfsson et al., 2020). According to the data of Mcafee (2021a), due to the pandemic, the number of connected devices at home increased 22% globally and 60% in the US.

It is debated whether remote work will become the new normal or whether the growth of remote work during the COVID-19 is only one peak in history (Leonardi, 2020). As stated earlier, permanent changes are expected. At least, the number of remote workers is unlikely to return to the 2019 level. Since the remote work experiment has seemingly gone better than expected, it is likely that the workforce will not be distributed as before (Ozimek, 2020).

2.2.3 The types of remote work

As it has been stated earlier, remote work can be divided to various forms of work such as working from home, airport or hotel. Furthermore, as the statistics (Office for National Statistics, 2020) prove, some employees work mainly remotely while some occasionally work remotely. These facts should be taken into account in the research. The starting points of remote workers have been different. Before COVID-19, many have not been working remotely at all (Office for National Statistics, 2020). This, along with budget and time issues (Sarginson, 2020), leads to the fact that some have had better starting points for remote work than others depending on their own and their companies' backgrounds.

Mokhtarian (1991) divides remote work to home-based and non-home-based type. Home-based type may involve running a business, bringing work home after office-based work, or working exclusively at home. Non-home-based type may involve working from a location other than primary office or home, field work such as sales work, working during traveling, or managing a branch office. Regarding the last one, it is stated that branch managers usually work remotely since their bosses, or supervisors, are at different locations. However, other employees of branch offices do not work remotely since their supervisors are present (Mokhtarian, 1991).

In the following chapters, no clear line has been drawn between home-based and non-home-based remote work. It is somewhat seen as a secondary subject for the purpose of the research. However, typical threats of different types have been raised. For example, using public wi-fi is a general procedure in public cafes (i.e. non-home-based remote work), and this procedure might create security threats (Curran, 2020). It could be said that, as COVID-19 has forced people to avoid traveling and stay at home, most remote work can be assumed to be home-based.

2.2.4 Typical applications

For the context, this chapter mainly focuses on today's typical applications utilized in remote work. In general, remote work is enabled by various digital technologies that allow communications via text, audio and video as well as the real-time editing of data and documents (Leonardi, 2020). In addition, virtual private networks (VPN) are enabling factors of remote work that also add security to the remote systems.

Regarding digital communications technologies, Leonardi (2020) reviews the change among user bases of Zoom, Microsoft Teams and Slack. The number of daily Zoom users increased by 67 percent in March 2020. The number of daily Teams users, in turn, increased by 120 percent from November 2019 to March 2020. In the first quarter of 2020, Slack received 40 percent more paying customers than in the previous quarter (Leonardi, 2020).

VPN, as Trzupek (2020) states, is a mechanism needed for employees to access organization's network and work remotely. Through encryption and IP address disguising, security is provided and operations can be performed as if the employee was directly connected to a particular private network (Trzupek, 2020). The usage of VPNs has increased remarkably during 2020 (Trzupek, 2020; NCSC & CISA, 2020).

Bloom, Davis and Zhestkova (2020) express that COVID-19 has affected technology innovations so that new applications that support working from home, as they express it, have increased their share of patents in 2020. They believe that more improvements may be expected regarding working from home technologies and tools (Bloom, Davis & Zhestkova, 2020).

2.3 Phishing on remote work

This chapter aims to answer the research question based on literature. Some known issues based on earlier literature and also some new potential issues are discussed. First, the major phishing issues regarding the ongoing COVID-19 situation are examined. Answers to the research question are sought, but it is noted that the ongoing situation has also offered attackers other opportunities beyond exploiting phishing on remote work. Second, the major phishing-related threats that can be stated to be due to remote work are reviewed. Threats can be changed means by attackers or changed operations by individuals or organizations. What the threats have in common is that they pose some kind of danger. A table of those threats has also been compiled, which to some extent summarizes the results of the literature review. Regarding the research question, the focus is on presenting the potential threats. However, towards the end of the chapter, some methods to defend against new threats are described.

Since the early days of phishing, successful attacks have inspired attackers to continue and also expand (Jakobsson & Myers, 2006; Rekouche, 2011). Thus, by protecting yourself from phishing you do not encourage phishers and, therefore, you are protecting others. Since the early days, phishers have been perfecting their attacks. Although individuals are educated to protect themselves, phishers probably have the same information and are educated as well (Jakobsson & Myers, 2006). Thus, it is no wonder that with the increase in remote work, in the midst of COVID-19 chaos, the number of phishing attacks has increased (NCSC & CISA, 2020; Ahmad, 2020).

It should be mentioned that COVID-19 does not appear in phishing only to exploit remote work in attacks. Phishers have also taken advantage of the widespread panic and individuals' thirst for information in order to create hard-to-resist scam messages (Ahmad, 2020; NCSC & CISA, 2020). This is notable since the possible, somewhat proven, increase in losses caused by phishing cannot be claimed to be exclusively due to the increase in remote work. This poses a challenge to research and the evaluation of remote work's impact.

Another challenge, especially for future research, is to figure out which of the arisen threats are sustainable. Many threats are related to rapid deployment of systems and technologies. Over time, the problems associated with rapid deployment may be resolved and some of the threats may diminish or even disappear. Presumably, the general confusion among technology users (NCSC & CISA, 2020) will dissipate.

Sarginson (2020) states that, in general, employees are working on less secure devices and networks while working remotely. COVID-19 spread so fast that many organisations did not have resources or time to add needed security to working devices (Sarginson, 2020). National Cyber Security Centre (NCSC), the United States Department of Homeland Security (DHS) and Cyber security and Infrastructure Security Agency (CISA) (2020) have prepared an advisory which again highlights that, during the year 2020, the topics of phishing messages have often been related to COVID-19. However, they also raise some issues that are very much related to remote work. The attackers have exploited commonly known vulnerabilities in VPNs, remote work tools and software. Phishers have sought to exploit widespread communications platforms such as Zoom and Microsoft Teams by sending emails that include attachments with the words 'zoom' and 'teams' in their names (NCSC & CISA, 2020). In practice, this could also be utilized by sending victims links that appear to be invitation links to Zoom or Teams meetings but are actually spoofed URLs. The effects the increase in remote work has on cyber security might be more obvious, as it can be shown that the increase has been exploited, but the effects on phishing require further research.

There are some prime examples how COVID-19 has been utilised in phishing. In 2020, between February and March, COVID-19 related spear phishing attacks increased 667% (Trzupek, 2020; Bissette, 2020). The increase is widely related to confused users and the aforementioned thirst for information. Although the confusion should dissipate and the thirst for information should decrease over time, the increase is worrying, as the phishers tend to expand and perfect their attacks.

Based on literature review, the following table (TABLE 1) summarizes the potential phishing threats that are specific to remote work. Especially, the table presents the phishing-related threats that are not caused by COVID-19 alone but are potentially, or proven to be, specific to remote work.

TABLE 1 The potential phishing threats that are specific to remote work

Threat	Explanation	Reference(s)
New technologies and confusion	The attackers have already taken advantage of rapidly growing new technologies such as communications platforms (Zoom, Teams, etc.) and VPNs. Regarding new technologies, the confused technology users can be seen as easy targets for phishing.	NCSC & CISA, 2020
Lack of security installation	Employees working on less secure devices and networks while working remotely.	Sarginson, 2020
Lack of support	Remotely working employees should know how to detect and react to phishing scams. Support exists but may be more difficult to access.	Ahmad, 2020
The huge spread of spear phishing	Strongly linked to confusion. Attackers exploit confused users. In 2020, between February and March, COVID-19 related spear phishing attacks increased 667%.	Trzupek, 2020; Bissette, 2020
Reluctance to take advantage of technologies	Reluctance to use certain new technologies might lead to missing important information.	Beaudry & Pinsonneault, 2010

New technologies have confused employees and individuals. New technologies refer to technologies that individuals have had to spend their time exploring. Attackers have taken advantage of the new technologies directly by emails that are sent with attached files that appear to be related to new technologies such as Zoom or Teams (NCSC & CISA, 2020). Furthermore, attackers have taken advantage of the new technologies indirectly by timing the attacks to coincide with confusion due to the technologies. In remote work, especially since switching to remote work was forced in 2020, there seems to be lack of security installation (Sarginson, 2020) and lack of support (Ahmad, 2020). A surprising need for new deployments may cause companies to take shortcuts (Trzupek, 2020). In 2020, spear phishing has spread remarkably (Trzupek, 2020; Bissette, 2020). During the year 2020, phishers have widely exploited the demand for COVID-19 related information in their attacks (Ahmad, 2020; NCSC & CISA, 2020). When it comes to spear phishing, it might be debatable whether remote work has contributed to growth. As the primary goal is to present potential threats, the threat, however, is real. If there are any shortcomings in technology use, security installations or IT support, spear phishing especially poses a great threat to individuals and organizations.

Regarding the issue with new technologies, the increase in the usage of the VPNs simultaneously with the increase of spear phishing possibly causes a need for more developed VPN usage monitoring (Trzupek, 2020). It is especially important to control the remote logins in the current state. MFA (multi-factor authentication), strong passwords and employees' remote work actions will have a strong impact on organizational security (Malecki, 2020). Guidance and education on how to make home routers and servers as secure as possible and how to manage wi-fi accessibility are major factors in securing the entire businesses. If employees inadvertently or recklessly use public wi-fi, they expose themselves to man-in-the-middle attacks (Curran, 2020).

Earlier research reveals the effect that emotions have on technology use. The effects of emotions require further glance, since various emotions such as confusion related to new technologies have already been discussed and more of those such as anxiety and pleasure related to IT use will be discussed in chapter four. Beaudry and Pinsonneault (2010) have examined the relations of different emotions and IT use. For example, pleasure is positively related to the intention to use and the intention to continue to use. On the other hand, anxiety is negatively related to the intention to use (Beaudry & Pinsonneault, 2010). This applies to the era of remote work and new technologies. The more pleasant the employee feels the use of a certain technology the more likely (s)he will use it and continue to use it. On the contrary, if the employee does not feel pleasant using the technology, (s)he might be anxious to ask for help through that particular technology. However, it may not always be a matter of a sense of pleasure. Therefore, Beaudry and Pinsonneault (2010) provide a wide range of information regarding different emotions and their relations to IT use.

The remote work increase is another new technological revolution. Revolutions of this scale affect individuals in different ways. Brown, Fuller and Vician (2004) have studied anxiety in the context of computer-mediated communication. In this context, anxiety is negatively related to the attitude towards using a computer-mediated communication tool (Brown, Fuller & Vician, 2004). In their study, due to the era and organizational environment of that time, the focus is largely on email use, which was quite a new phenomenon at that time. Although technology has evolved tremendously, that period can be seen as similar to the current era of remote work. New technologies still constantly confuse individuals, especially recently. Anxious users of Teams, for example, might have a negative attitude towards using Teams to ask for support. In case of a remote work security threat, the user might miss out on important information.

3 EMPIRICAL RESEARCH METHODOLOGY

This chapter first explains the goal of the empirical research. Second, the processes of examining various methodologies and preparing the empirical research are described. This is followed by a brief description of the processes of data collection and analysis.

3.1 Goal

To begin with, the empirical research aims to support the findings on literature. Basically, the literature review raised new questions. There is evidence of the increase in the number of phishing attacks. Have respondents noticed this? Are the potential new threats the same as those highlighted in the literature review? Are there some other kind of threats? The purpose remains on answering the research question but the aforementioned questions supported the preparation of the empirical research. COVID-19 forced a large number of workers to switch to remote work in March 2020. As qualitative research rather explores meaning than generalizes and creates hypotheses (Mason, 2010; Crouch & McKenzie, 2006), and as the resources are limited, the research does not aim to achieve any generalizations regarding, for example, whether the employees have received a higher amount of phishing messages while working remotely. This topic is addressed but the results are not generalized. Instead, the purpose of the empirical research is to uncover individual experiences during the year of remote work and to examine the changes experienced compared to the time before March 2020. In other words, instead of generalizing or creating hypotheses based on data, experiences are reviewed and reported, and proposals are made for further research.

3.2 Preparation

Various methodologies were considered in conducting the empirical research. The four considered options were as follows: field experiments, surveys, interviews and online material research. At this stage, all research regarding the topic is valuable. The option of online material research was crossed out in an effort to get the most recent responses possible. In the foreseeable future, experimental research would be valuable because it could enable measuring dangers that have not yet become exact threats (Finn & Jakobsson, 2007). However, with the given schedule and resources, interviews were seen as a reasonable approach for the research. Presumably, compared to a questionnaire, it is easier to stay on topic when interviewing a person face to face. In questionnaires, respondents' understanding of phishing may lead to underestimations or overestimations of damages or risks (Finn & Jakobsson, 2007). In general, the lack of awareness among cyber crime victims often leads to the underestimation of the amount of incidents (Fafinski, Dutton & Margetts, 2010). These challenges are not insuperable but, after all, the interviews were seen as a practical approach. Semi-structured interview enables further explanations in case that a respondent does not understand some question or concept.

The semi-structured theme interviews were organized in March 2021. The interview preparation included two steps: preparation of the structure and selection of the interviewees. First, the structure of the interviews was conducted after the literature review was written and some questions regarding occurred potential threats were included. The structure was conducted so that in the beginning the interviewees were led to talk about cyber threats in general and, to end up with, they were led to talk about phishing. Second, the interviewees were selected. The following requirements were set for interviewees:

1. The interviewee has experience from both office work and remote work.
2. The interviewee is familiar with the concepts of phishing and cyber security.
3. The interviewee uses email on a daily basis at work.

For the interview, individuals who had worked both remotely and in the office were selected. The interviewees were aged 24-28. Such a slight age range was not planned but it was not seen as a significant drawback because other requirements were met. In addition, some research states that, when it comes to the attitude towards technology, the experience of using the technology matters rather than the age of user (Czaja & Sharit, 1998). In addition, the pleasure to use a technology is positively related to the intention to use the technology (Beaudry & Pinsonneault, 2010) whereas anxiety to use a communication tool is negatively related to the attitude towards using the communication tool (Brown, Fuller & Vician, 2004). As the experience of using today's remote work technologies is, in any case, thin at most, the author aimed to select respondents that are somewhat familiar with technologies specific to remote work. The experienced pleasure while using technologies was not a requirement carved in stone, but it was, however, noted during interviews that each respondent felt quite pleasant using technologies specific to remote work. The author believes that, in general, this will lead to more detailed responses related to respondents' own experiences. Regarding technology use, the selected interviewees have diverse backgrounds as half of them have studied IT and, furthermore, some were a lot more experienced in using the communication technologies, for example, than others. However, all the respondents had academic backgrounds and some experience about relevant technologies due to the aforementioned requirements. Discretionary sample was used in order to get attentive responses but a greater dispersion in age and workplace roles would have added a kind of value to the research. When selecting the interviewees, it was ensured that each of them used email on a daily basis. The interview structure can be seen in appendix 1 (in English) and appendix 2 (in Finnish). All interviews were conducted in Finnish, as it was the mother tongue of each interviewee. Interviews were conducted as one-on-one interviews so the interviewees did not know the identities of each other.

A semi-structured interview was selected as a method. In general, the semi-structured interview is always a suitable and flexible solution for a small-scale research (Drever, 1995). The two major reasons that led to selecting this method were as follows:

1. The possibility to define concepts and change the vocabulary based on the respondent's receptivity.
2. The possibility to ask specific questions based on the respondent's experiences.

First, the information security knowledge of the interviewees varied. Each of them generally understood the concept of phishing. This was proven as they were asked to define the concept. However, some needed more guidance than others. In addition, the vocabulary used by interviewer varied a bit depending on background of a particular interviewee, which is an acceptable technique in semi-structured interviews (Newcomer, Hatry & Wholey, 2015). Second, the experiences of the interviewees varied a lot. Instead of only asking sweeping questions such as 'what security threats have you experienced at your work' and waiting silent as the interviewee lists all the threats, some follow-up questions were also asked based on the experiences. Semi-structured interviews enable asking follow-up queries (Newcomer, Hatry & Wholey, 2015).

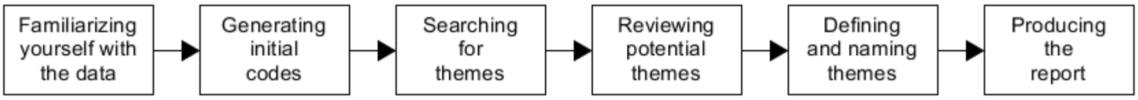
3.3 Data collection and analysis

Qualitative data were collected through six interviews. The main goal of the empirical research is to answer the research question. To answer that, the empirical research aims to both support and challenge the findings of literature. As the generalizations are not sought, six was seen as an acceptable number. For instance, Guest Bunce and Johnson (2006) state that through six interviews enough data can be gathered to support themes. It is the connections among codes that may not be as apparent with a number this low (Guest, Bunce & Johnson, 2006). Through six semi-structured interviews, repeated responses were received, and the responses remained relevant. The findings of literature were both supported and challenged. Interviews were organized in March 2021, approximately a year after the COVID-19 forced a remote work expansion. Four interviews were arranged via Zoom and two interviews face-to-face. All interviews were recorded and transcribed. After that, transcriptions were analysed through a proven method. In this chapter, the process of data collection and analysis is divided into sections and described in detail.

The interviews lasted 35 minutes on average. Thus, the amount of data to be examined was approximately three and a half hours. First, the same background questions were asked from respondents. Next, the structure was followed but some differentiating questions were asked based on respondents' answers and experiences. For example, if it turned out that the respondent's work email had an add-on to combat or train against phishing, some further questions regarding this were asked.

The interview data was analysed through thematic analysis which is "*a method for systematically identifying, organizing, and offering insight into patterns of meaning (themes) across a data set*" (Braun & Clarke, 2012; originally, Braun & Clarke, 2006). As a simple and flexible method, it complements the data collection method used in this research. Thematic analysis may, for example, produce answers to questions that are not directly asked and only become apparent during the analysis process (Braun & Clarke, 2012). Since the semi-structured interviewing style was used in data collection process, meaning that different questions were asked from different respondents, thematic analysis makes it possible to compare the responses with each other. Furthermore, a flexible method is used since the purpose is to support or, on the other hand, challenge the literature review findings.

Braun and Clarke (2012) offer a six-phase approach to thematic analysis. The phases are as follows: (1) Familiarizing yourself with the data, (2) Generating initial codes, (3) Searching for themes, (4) Reviewing potential themes, (5) Defining and naming themes, and (6) Producing the report (Braun & Clarke, 2012). This approach, visualized in the following figure (FIGURE 1), summarizes the analysis process.



Familiarizing yourself with the data → Generating initial codes → Searching for themes → Reviewing potential themes → Defining and naming themes → Producing the report

FIGURE 1 A six-phase approach to thematic analysis (Braun & Clarke, 2012)

As a novice researcher, in addition to Braun and Clarke (2012), the author utilized the guidelines provided by Maguire and Delahunt (2017). Following aforementioned steps, first, the entire data was carefully read. Second, the codes were generated to capture the relevant parts from the large amount of data. In practice, this phase was executed by placing data to Excel (Bree & Gallagher, 2016; Maguire & Delahunt, 2017) and writing codes (i.e. notes) while examining and comparing the responses to certain questions. Third, themes were searched and found. In practice, themes were formed from repetitive codes but also, from anomalous codes that were relevant for the research question. As the steps progressed, an attempt was made to find relevant information about the large amount of data. Next, the themes were further reviewed and the headlines of chapter four were finalized. Major questions asked while finalizing the themes and headlines were whether potential themes included some useful information regarding the research question and whether there were enough data to support the certain theme (Braun & Clarke, 2012). Other questions were also asked following the instructions for phase four as in Braun and Clarke (2012). Lastly, the results were written. To justify and strengthen themes, multiple quotations were included. This also aims to make the results more readable, vivid and detailed (Newcomer, Hatry & Wholey, 2015).

The themes might overlap. For example, the flow of information is strongly related to both communication technologies and experienced threats, and one quotation or code might give valuable data to each theme. However, there were enough data and differences to make each their own themes. Furthermore, the amount of data supporting each theme varied. This has been addressed in the following way. The more data there was about the theme, the more comprehensively it has been reported.

Considering the context, repetitive patterns but also anomalies have been highlighted. The results of the analysis process are discussed in the next chapter. The patterns that emerged in several interviews have been reported broadly while individual responses that significantly appear either supportive or provocative to previous results have been discussed briefly.

To end this chapter, a deeper look in the background information should be taken. The following table (TABLE 2) briefly summarizes the ages and working industries of interviewees.

TABLE 2 The interviewee background information

Respondent	Age	Working industry
R1	24	Construction
R2	28	Energy
R3	27	Construction
R4	24	IT
R5	27	Finance
R6	25	Education

As mentioned before, a greater dispersion in age and roles could have added some value to the research. However, attentive responses were sought and younger people tend to have a better IT knowledge. In addition, three out of six respondents have a history of IT studies and three others have become familiar with technologies important to this research through their work. The respondents were also asked to describe the amount of remote work they have done before and after March 2020. Five out of six respondents have practically switched to remote work in March 2020 and are still working remotely in March 2021. The only respondent that is not working mainly remotely works in the construction industry in a position that apparently requires a lot of presence. However, even this respondent worked half the time at home in the spring of 2020.

4 RESULTS

This chapter presents the results of the empirical research. Chapter 4.1 generally reviews the results without focusing on details. It serves as a bridge between the literature review and the empirical research. In chapter 4.2, the themes found through analysing the interview data are discussed one by one. Each subchapter examines a certain theme found and created based on the thematic analysis. In practice, the themes related to research question that were discussed most during interviews are now reviewed. From approximately three and a half hours of interview data, the most illustrative quotations were aimed to be included in this chapter.

4.1 Overview of results

In the beginning of each interview, the focus was on not leading the respondents to only discuss about phishing. Instead, they were asked about general cyber security threats that they had experienced at work. In this regard, all respondents mentioned phishing. In the middle of the interviews, respondents were asked to define phishing. All the respondents more or less knew how to define phishing. Although, they mostly described examples of attacks where phishing techniques are utilized instead of explaining the concept. All the respondents knew to tell that their companies had received phishing messages, one way or another. However, some had not received phishing messages at all to their individual (work) email. This was a major challenge in interviews: how to examine the changes in operations when respondents had such a light experience regarding phishing. Semi-structured interview, however, enabled the collection of experiences which varied a lot between respondents.

Based on the literature review, respondents were asked questions about new technologies, IT support and its accessibility, and the security education provided by their companies. Although these factors were widely discussed, based on interviews, they do not represent the greatest phishing-related threats for respondents. Instead, a major theme discussed as a threat was the decline in the flow of information. This is an important issue, also for a further research, and, therefore, it is reviewed as its own theme in the following chapter. Basically, other themes such as new technologies and IT support are also strongly linked to the flow of information and, therefore, the positive and negative aspects of each are examined. After all, the successful flow of information could prevent most phishing attacks or at least reduce the negative effects of the increase in remote work. The literature review did not discuss the flow of information. It is, however, strongly linked to the reluctance to take advantage of new technologies, which can be seen as a major factor behind the declined information flow.

Although generalizations cannot be made by this qualitative research, the interviews loosely supported the claim that spear phishing is an even greater threat than before. One respondent had received spear phishing emails for the first time in his/her career. Another respondent had received COVID-19-related spear phishing emails. Otherwise, there was hardly any data, and spear phishing is only discussed as one of the threats in chapter 4.2.2.

For their own part, the respondents did not experience the threat of phishing to be significantly greater than before. Some had heard that the number of phishing attacks has generally increased but could not confirm this for their part. The respondents mentioned examples in this regard:

> "I have not noticed the change in quantity or quality of phishing myself, but I have heard from colleagues that the number of attacks has increased." -R2

The danger of phishing is expected to be somewhat greater than before but, once again, this expectation is based on discussions with colleagues and general assumptions.

4.2 Themes

Based on the interview data, five themes were defined through thematic analysis. Defining and naming the themes was a difficult task since they contain different amounts of data. Threats were talked approximately half of the total time of the interviews. Thus, half of the data is related to experienced threats or potential new threats. The major threat, the flow of information, manifested itself strongly and, therefore, deserves to be a theme itself. The flow of information is reviewed in subchapter 4.2.1. Otherwise, the experienced threats varied between respondents. These other, experienced or seen as potential, threats are described in subchapter 4.2.2. In defining other themes, potential themes were compared to the ones discussed in literature review. Regarding the research question, the positive and negative aspects, and the changes in threats as well as other changes should be taken into account. The chapter of experienced threats is followed by one-by-one reviews of the themes of new technologies

(4.2.3), IT support (4.2.4), and the first actions in the defence (4.2.5). Each of these themes is a potential threat, but the changed working methods are also examined. In this way, treating each as their own theme, thematic comparisons can be made between the literature review and the results of the empirical research. In addition, some interesting details and quotations can be brought up.

4.2.1 The flow of information

A major theme that was discussed in all interviews, and was also seen as a definite threat, is the decline in the flow of information. Although this issue has been tried to be fixed by arranging meetings more often, the unspoken, or inadvertent, flow of information is diminished. In this regard, the following citations were captured:

> "After all, it has been a problem in many companies that knowledge, or an unspoken knowledge, does not flow. Remotely, people do not exchange stories about certain things. Some can be in the dark about certain things if those are not told separately. You will definitely miss a lot of information." -R1

> "In office work, more gossip and such was discussed, but important things were also shared. Not everything is shared when you are working remotely." -R2

> "Recently, meetings have been held more often because information does not flow through corridors or coffee rooms." -R6

Regarding the growing threat of phishing, some saw this as a significant factor but, above all, the decrease in the flow of information was considered an important factor in the fluency and meaningfulness of the work. Regarding the latter citation, the efficiency of work might suffer because more meetings are required to be arranged. Phishing and other information security threats, however, are only one part of the things that need to be discussed in those meetings. In general, when it comes to the information security threats, the information still flows. One respondent described the phenomenon as follows:

> "Conversation between co-workers is a bit decreased when you can't see others in the office physically, making it a lower threshold to discuss things when you are there face to face. Now it is a little higher threshold perhaps to contact by electronic tools -- even now if there is any information security threat or such, then the information passes. But whether those issues are discussed so much with co-workers directly is probably a bit decreased." -R5

It should be comforting for organizations that security-related information is still believed to reach employees. However, certain individuals might be in danger of missing important information. Such information can, at best, prevent a security breach. The reason why some individuals might miss the important information can be related to, for example, the pleasure of using technologies or the reluctance to ask for help. The emotions and their relations to IT use were described in chapter 2.3 in which some relevant literature was also given (e.g. Beaudry & Pinsonneault, 2010). Regarding the potential effect of emotions, one respondent stated as follows:

> "We also had some employees in their fifties who did not like using Teams and did not send messages there. Not everyone necessarily likes to use new technologies and they might be anxious to use those. Alone at home they may not agree to ask anyone. At work, they could ask for help, but maybe they are alone at home and have to manage on their own." -R1

Based on the above quote, and the fact that the age was mentioned, older people might be in greater danger of missing information. This is somewhat in line with research, although it was mentioned earlier that, when it comes to the attitude towards a certain technology, the experience of using the technology matters rather than the age of user.

This theme requires further research as new important issues have arisen. In the literature review, the relations of different emotions and IT use are reviewed. For example, pleasure is positively related to intention to use and intention to continue to use. This applies to this theme. The more pleasant the employee feels the use of a certain technology the more likely (s)he will use it and continue to use it. On the contrary, if the employee does not feel pleasant using the technology, (s)he might be anxious to ask for help through that particular technology. As mentioned in the literature review, in the early days of email, anxiety among users resulted in lower probability of using email. Similarly, anxiety caused by new technologies might result in the reluctance of taking advantage of these technologies. In other words, employees who are already anxious do not ask for help with their problems. However, it may not always be a matter of a sense of pleasure or anxiety. Therefore, the question remains, what emotions exactly cause the resistance to ask for help or support through technologies used in remote work.

4.2.2 Experienced threats

As mentioned before, the structure of the interview was conducted so that in the beginning the respondents were led to talk about cyber threats in general and, to end up with, they were led to talk about phishing. However, when being asked what kind of cyber-threats they have experienced at work, all the respondents mostly discussed phishing-related threats. In addition, phishing emails or suspicious emails were the only threat mentioned by all respondents. Some had to rethink the suspicious messages they had received, but it became clear that everyone had at some point received phishing messages. Three out of six respondents stated that they had received suspicious phone calls that were clearly phishing attacks. In general, the respondents could not amplify whether the number of attacks had increased. However, the number, as well as a threat in general, was believed to be higher than before.

Experienced threats included traditional email-based phishing and phone phishing. Some of the attacks can be considered to be spear phishing. In chapter 2.3, it was stated that, during the year 2020, the increase in spear phishing attacks was huge. This statement was slightly strengthened by interviews as two respondents could tell that they had received spear phishing emails. At least the other one had received spear phishing emails for the first time in his/her professional career whereas the other one was not completely certain whether (s)he had received those before. Regarding the huge spread in COVID-19-related spear phishing, presented in the literature review, the other one of the respondents that had received spear phishing stated that it had nothing to do with COVID-19. The respondent stated that due to his job duties, phishing messages are generally very rare. In this regard, the following relevant point was also stated:

> "In our company, those who are more connected to other people, for example, through buying materials or making purchases, are more in contact with people so they face significantly more of these phishing attempts." -R3

According to the experiences of this respondent, phishing attacks had almost exclusively been such that an email is received that allegedly comes from a colleague who has in fact been the victim of phishing. Those kinds of frauds are challenging to observe, as the respondent states:

> "It is sent from a coworker's email and it just has some link so it is, so to speak, easy to open and you do not think it could be a phishing message." -R3

However, in general, the respondent had not noticed a significant change in the quality or quantity of phishing messages. The other respondent had received COVID-19-related spear phishing emails. (S)he stated that they had received so called corona bonus messages at work. The recipients had been lured to click the link in messages claiming that they had been awarded an additional monetary reward.

In general, respondents experienced, especially if their employment was relatively recent, that there are a lot of different systems. The number of systems is even higher today when there are new systems due to the needs of remote work. This creates the need for more usernames, passwords, and logins, which, in turn, further complicates the implementation of security and also the protection against phishing. In this regard, one respondent stated as follows:

> "When there are such many different systems in use today, I think there is a greater risk that your own username and password may spread, especially if you use the same username and password in different systems." -R2

The following table (TABLE 3) compiles the threats respondents have faced. In addition, their observations regarding the experienced changes in quality or quantity of phishing have been raised. Although the observations are uncovered, definite generalizations cannot be made. This is due to the sample size and the rarity of phishing messages in general. What the observations aim to achieve is that some respondents have noticed or experienced changes regarding phishing threats in remote work but the experiences are different.

TABLE 3 The threats experienced by respondents

Respondent	Experienced threats	Other observations
R1	suspicious emails, spear phishing	No definite changes in quality or quantity of phishing. COVID-19 has been exploited.
R2	suspicious emails, phone phishing	No definite changes in quality or quantity of phishing. Having more systems creates a greater threat.
R3	suspicious emails, potential spear phishing emails	No definite changes in quality or quantity. Spear phishing is potentially increased.
R4	suspicious emails, phone phishing	No changes at all in quality or quantity.
R5	suspicious emails, phone phishing	No definite changes in quality or quantity.
R6	suspicious emails	No definite changes in quality or quantity.

Basically, the table presents the threats respondents have already faced, and their opinions regarding the threats in general. The observations do not include the ones related to the decline in the flow of information as it is already stated that the particular issue was discussed in all interviews. Although most respondents have not noticed definite changes in quality or quantity of phishing they have encountered, the general opinion seems to be that the risk of being scammed is greater than before. One way or another, the decline in the flow of information was also discussed as a threat in each interview.

4.2.3 New technologies

As it was suggested in the literature review, new technologies have confused users and attackers have utilized this issue. When respondents were asked about completely new technologies or technologies that have been increasingly used, communication technologies were the main topic of discussion. Microsoft Teams was the primary communications platform for five out of six respondents. Zoom was also in use alongside Teams but it was stated by one respondent that, according to their safety instructions, the work should not be discussed there. One respondent mentioned Slack as their major communications platform for messaging and Google Meet as their major platform for video meetings. Following table (TABLE 4) summarizes the communication technologies in use.

TABLE 4 The communication technologies in use

Respondent	Primary communication technology
R1	Teams
R2	Teams
R3	Teams
R4	Slack, Google Meet
R5	Teams
R6	Teams

As discussed earlier, the decline in the flow of information due to a decreased communication was frequently raised in the interviews. Communication technologies did not provoke resistance in respondents and were discussed in a rather positive tone. However, the above-mentioned quotation "*we also had some employees in their fifties who did not like using Teams and did not send messages there*" highlights the fact that the resistance exists. Some view change positively and some negatively. According to the responses of the organized interviews, the resistance is lower among younger individuals. One respondent raised the following as a positive point:

> "Complicate things are easier to discuss face-to-face, but simple things might be even easier to be asked in Teams, since the respondents may answer when they have time to do so." -R6

This might be one of the positive aspects of using communication technologies: the fluency of your own work. However, how has this affected phishing? If the question asked concerns phishing, a downside may be at least that, once the response is received, it may already be too late.

4.2.4 IT support

Contrary to the literature review, it may be suggested that respondents have not had problems accessing IT support. The respondents were asked about the accessibility of IT support and it was exclusively stated that the support is received quickly enough. Each respondent had contacted IT support or IT department over the past year and the support was received immediately. Each respondent had strong confidence in the IT support of their own company. However, it is believed that this is necessarily not the case in every company. One respondent stated as follows:

> "In my own company, IT support has been perfectly accessible, but it might still be easier for criminals worldwide, for example, to contact workers and succeed in phishing because remote work has increased." -R5

In chapter 2.3, it is noted that both remote work and COVID-19 itself have been utilized in phishing. One respondent stated that the time has been favourable for sending COVID-19-related, or any other kind of, messages due to general confusion. In some companies, there might be a real lack of support.

This theme and the related interview questions concerned corporate departments of IT support. According to the responses, these so-called official departments provide perfectly accessible support. However, it is only one way to receive support. This theme is also strongly affected by the decline in the flow of information. As it is reviewed in chapter 4.2.1 and as it is discussed in the following chapter, the amount of face-to-face lower threshold discussions has decreased. As a result, the amount of support received from casual discussions with colleagues has decreased. Support can also be obtained from colleagues and, in this regard, the remote work has created challenges for mutual support between colleagues.

4.2.5 The first actions in the defence

A question that was not considered in the literature review or included on the original interview structure but was, however, later added as it seemed to differentiate the respondents, is as follows: *if you receive a suspicious email, what do you do first*. Furthermore, it was noted that the transition to remote work had affected the first actions.

The responses were as follows. Two of the respondents work in companies that use Hoxhunt (briefly described in chapter 2.1.4) as an email plugin, so their first step is to report the suspicious email. One respondent begins by asking colleagues for support and another one mentions that colleagues have usually already discussed about the same message. One of the respondents said (s)he would not take action when (s)he noticed the suspicious message since those have been so easy to notice and, similarly, another explained that (s)he usually moves the message to the spam folder.

> "Sometimes I mention (scam messages) to co-workers, sometimes I just simply delete those messages from there." -R4

Two respondents in the companies using Hoxhunt regarded the plugin as a positive addition to their work. In the interviews, it was asked if Hoxhunt was activated in respondents' companies due to COVID-19 or the remote work expansion. Both replied in the negative, although one of them mentioned that COVID-19 may have confirmed the idea of deployment. While generalizations cannot be made, the existence of Hoxhunt clearly encourages employees to take some action in response to a suspicious message. Of all the companies of respondents, only in the ones using Hoxhunt the information regarding the scam messages reaches IT support at a relatively early stage.

Although the first actions taken in case of receiving a suspicious message varied, all respondents sometimes discuss phishing emails with colleagues, usually in a laughing tone. The laughing tone is due to the fact that phishing messages are not generally seen as significant threats. The conversations can be quite casual, the amount of which has decreased in the remote work era. Some individuals, however, may need support. The decline in the flow of information, and a possible higher threshold to contact through technology tools, may cause poor decisions in case of receiving suspicious messages. Those individuals who are normally eager to ask for help from their colleagues, face various challenges due to the remote work. Their first actions after receiving suspicious messages may be affected by the lack of support or the difficulties in obtaining support.

5 DISCUSSION AND CONCLUSIONS

5.1 Discussion

The literature review examined phishing in the remote work environment. The research question was as follows: *how has the increase in remote work affected phishing?* This question was examined from various perspectives. To begin with, the number of phishing attacks has increased. This is stated to be due to both the increase in remote work and the ongoing COVID-19 situation which makes people eager for new information. When it comes to threats caused by remote work increase, based on literature, following results were found. First, technologies that are new for employees have been exploited in attacks. For example, attackers have taken advantage of widespread communications platforms such as Zoom and Microsoft Teams. In addition, the confusion caused by new technologies has been utilized by attackers. Second, employees tend to work on less secure devices and networks while working remotely. In addition, support in problematic situations may be harder to access. Spear phishing attacks have increased dramatically, which is related to new technologies and confused users. COVID-19 has provided new means for spear phishing attacks but those might also be a great threat regarding remote work. The impact of the emotions evoked by the technological revolution was examined. In this regard, the reluctance to take advantage of new technologies is another potential threat. Users' emotions are related to their intentions to use systems. If the use of a system is unpleasant, the threat of missing information is higher.

Empirical research aimed to answer the research question and support as well as challenge the findings of the literature review. A major finding of the literature review, the increase in the number of phishing attacks, was supported by multiple respondents. Altogether, the number of phishing attacks touching the respondents was quite low but the general increase was definitely observed. There was no clear answer to how much this is due to the increase in remote work. The issue that occurred in most interviews is that the flow of information has decreased. This was seen as a detrimental factor to the fluency of work that could also expose individuals to security threats. On the other hand, it was partially observed that in case of a security threat the information still passes. In this case, a threat is supposed to be something that maybe concerns the whole organization. The number of casual discussions is lower than before. Thus, as the daily debate has decreased, so has the talk of security issues. The support between colleagues might decrease and the first actions and decisions in case of an attack might be poor as the information does not flow as before. Regarding the flow of information, it is important to acknowledge that the more pleasant the employee feels the use of a certain technology the more likely (s)he asks for help using that technology.

The differences between the results of the literature review and the empirical research suggest that, at this point and with these resources, the potential threats can be described and the protection against threats can be strengthened. However, prioritizing the threats is difficult since there are so many differences in findings. The longer the employees continue working remotely the more comfortable they should feel using the remote work technologies. The resistance against new technologies should be minimized in order to minimize security threats. However, care and caution are required and employees should not rely too much on technology or their own awareness. There is a demand for IT support and, according to the respondents, it has been easily accessible.

Threats could be divided into internal and external threats. Internal threats are caused by the operations performed by the organizations and their employees, whereas external threats are caused by the operations performed by attackers. Internal threats related to remote work are the decline in the flow of information, the reluctance to take advantage of new technologies, general confusion, the possible lack of support and the possible lack of security installation. External threats are the increase in attacks, the increase in spear phishing and the utilization of new technologies. The division is displayed in the following table (TABLE 5).

TABLE 5 Division into internal and external threats

Internal threat	**External threat**
The decline in the flow of information	The increase in the total number of attacks
The reluctance to take advantage of new technologies	The increase in the number of spear phishing attacks
General confusion	The utilization of new technologies
The possible lack of support	
The possible lack of security installation	

When it comes to the phishing-related threats remote work has created, the research highlights that the decline in the flow of information is the greatest concern at this stage. As it was indicated in chapter four, the flow of information is related to most threats and was mentioned by each respondent. New methods to improve the flow of information should be considered. The threats overlap to some extent. By improving the flow of information, the significance of other threats is also reduced. In the future, it will be interesting to examine which of the emerged threats are sustainable and which are only momentarily caused by the increase in remote work and perhaps a momentary confusion.

The following table (TABLE 6) provides an updated overview of the potential threats posed by remote work (originally presented in chapter 2.3). The results of literature review are now compared to the results of empirical research. Empirical research managed to support especially two of the literature review findings: the confusion caused by new technologies and the reluctance to take advantage of new technologies. The confusion caused by new technologies and the reluctance to take advantage of those technologies are factors that contribute to the decline in the flow of information.

TABLE 6 Literature review threat findings in comparison with empirical research findings

Threat	Literature review	Empirical research
New technologies and confusion	The attackers have already taken advantage of rapidly growing new technologies such as communications platforms (Zoom, Teams, etc.) and VPNs. Regarding new technologies, the confused technology users can be seen as easy targets for phishing (NCSC & CISA, 2020).	All the respondents felt quite pleasant using new technologies. New technologies and confusion, however, are factors causing the decline in the flow of information.
Lack of security installation	Employees working on less secure devices and networks while working remotely (Sarginson, 2020).	All the respondents used email on a daily basis before COVID-19. Devices and networks are considered secure.
Lack of support	Remotely working employees should know how to detect and react to phishing scams. Support exists but may be more difficult to access (Ahmad, 2020).	Each respondent had strong confidence in the IT support of their own company. Accessibility is not a problem. Mutual support between colleagues has decreased.
The huge spread of spear phishing	Strongly linked to confusion. Attackers exploit confused users. In 2020, between February and March, COVID-19 related spear phishing attacks increased 667% (Trzupek, 2020; Bissette, 2020).	Some respondents had received the first spear phishing messages in their career/life during the remote work. Generalizations can not be made.
Reluctance to take advantage of technologies	Reluctance to use certain new technologies might lead to missing important information (Beaudry & Pinsonneault, 2010).	The reluctance to use communication technologies is a major factor causing the decline in the flow of information.

The empirical research found a few potential threats that had not been considered in the literature review. The number of systems is higher than before and, therefore, there might be a greater risk of username and password spreads. The first actions in the defense against phishing was discussed with each respondent. The decline in the casual conversations between colleagues may lead to poor decisions because some individuals are eager to ask for help from their colleagues.

5.2 Conclusions

The research was conducted in the following order: (1) the literature review, (2) the empirical research, and (3) the remaining sections. Based on the literature review, the interview structure was created. Thus, the findings of literature review were supported and challenged. As table 6 indicated, new technologies and consequent confusion, the lack of security installation, the lack of support, the huge spread of spear phishing, and the reluctance to take advantage of technologies are potential phishing-related threats in the remote work environment. The research succeeded in compiling an overview of various potential threats based on existing research and data. In addition, the empirical research highlighted some threats that may have not been raised earlier and deserve further research. The higher number of systems than before and the possibly poor first actions and decisions in case of an attack are noteworthy mentions. The major finding and theme of the empirical research, the decline in the flow of information, has been discussed broadly. The importance of this issue is emphasized by the following facts. First, it was mentioned by each respondent as a potential threat. Second, the flow of information appears to be strongly linked to other threats. Solving this issue might decrease the significance of other threats too.

Relevant to the subject, Robert Krug (the network security architect for Avast) has stated:

> "Computer viruses can spread just as easily as human viruses. Just as you would avoid touching objects and surfaces that are not clean, so should you avoid opening emails from unknown parties or visiting untrusted websites." (Raconteur, 2020)

During the ongoing pandemic, staying at home protects from some viruses but might expose you to other viruses. Falling for scams encourages phishers while responsibility and individual choices that promote protection prevent the spread of phishing. Both individual and organizational decisions affect the general security. Every organization and every individual can affect the profitability of phishing and the willingness of phishers to spread their attacks.

5.3 Contributions to research and practice

The effect remote work has on phishing is a topic that has not required much of research before. However, in 2020, as the number of remote workers multiplied, the threats involved were a cause for concern. This research aimed to compile those recently found threats, compare them to each other, and possibly find factors behind them. In addition to providing a comprehensive information package regarding phishing in remote work environment, the research manages to make two major contributions to research. First, the decline in the flow of information was found to be a great concern at this stage of remote work and new ways to improve that should be searched. Second, the research indicates that the confusion caused by new technologies and the reluctance to take advantage of those technologies fuel the information flow problem.

The major contribution to practice revolves around the same subject. To protect themselves from phishing attacks, companies should find new ways to improve the flow of information. The research indicates that information flow might be the greatest concern at this stage, as equipment security and the accessibility of IT support, according to the respondents, appear to be at an acceptable level. Especially, individuals who are reluctant to take advantage of new technologies form a risk group, and new methods should be invented to reduce the reluctance. The author believes that, at both individual and organizational level, efforts should be made to remedy this problem, as the effects of the problem may be societal. As the successful attacks inspire attackers to expand their methods, every organization and every individual is responsible for fighting phishing.

5.4 Limitations

The major challenge in the research was that finding reliable statistics regarding, for instance, losses caused by phishing is a challenge at the moment. Furthermore, it is almost impossible to evaluate what percentage of those losses is caused by remote work rather than COVID-19 itself. COVID-19 alone has caused chaos and transformed phishing attacks and, therefore, examining the influence of remote work, especially, will be easier when the state of affairs calms down.

When it comes to the limitations of the chosen methodology, respondents admitted having troubles remembering the events and practices of the previous year. To be fair, phishing messages seemed to be quite rare and these situations were not desirably memorable for them. On the other hand, this might indicate that employees have adopted new ways of working and are not longing for the old model.

The interviewees had somewhat similar backgrounds. Most of the interviewees had less than two years of work experience in their own field and no individuals at the highest level in their organization’s hierarchy were interviewed. Still, this was a somewhat measured choice. In the age group 24-28, it was easier for the author to find multiple interviewees. Having just a few older interviewees could have distorted the results. Most of the interviewees had experience in the IT field, either through work or studies, and they already had the basic knowledge regarding information security. Furthermore, younger individuals tend to have more knowledge of the information security issues which possibly allowed for more attentive comments. The empirical research was conducted through qualitative method and, therefore, no definite generalisations from sample were made. However, having a balanced group with different backgrounds would have opened up several perspectives.

5.5 Future research

All research considering the topic is valuable at this stage. The topic is fresh in its current scope and new information is constantly available. To begin with, it would be essential to find out, on a larger scale, whether phishing message recipients have been scammed more often while working remotely, compared to office work. Furthermore, the question remains, how much of that is due to the increase in remote work and not COVID-19 itself. Field experiments play an important role regarding whether the threat of phishing has increased or not. Statistical research would also be valuable in the future. Some potential phishing-related security threats caused by the remote work increase were highlighted in the literature review: new technologies, lack of security installation, lack of support, the spread of spear phishing and the reluctance to take advantage of new technologies. Future research could pay special attention to these issues, their effects on security and their sustainability. The research examined, at a relatively early stage, how the huge increase in remote work has affected phishing. As the amount of work performed remotely will presumably stay somewhat high compared to the time before COVID-19, future research could focus on the persistent threats that will be proven to pose a continuing threat to remote workers even when, so to speak, the situation returns to normal.

This research contributed to the general research in the field by strengthening the importance of information flow. There were two found factors contributing to the decline in the flow of information: the confusion caused by new technologies and the reluctance to take advantage of new technologies. Future research could take a position on preventing these. Presumably, over time, the confusion will dissipate. Therefore, additional research could be conducted, especially, to explore the reluctance to take advantage of technologies and the reasons that cause the reluctance. Future research, as well as organizations and individuals, should focus on ways to reduce reluctance to use technologies and improve the flow of information. Above all, any additional research aiming to improve the security is valuable.

REFERENCES

Abbasi, A., Dobolyi, D., Vance, A., & Zahedi, F. M. (2021). The phishing funnel model: A design artifact to predict user susceptibility to phishing websites. Information Systems Research.

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker Jr, J. F. (2010). Detecting fake websites: The contribution of statistical learning theory. Mis Quarterly, 435-461.

Ahmad, T. (2020). Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. Available at SSRN 3568830.

Aldawood, H., & Skinner, G. (2018, December). Educating and raising awareness on cyber security social engineering: A literature review. In 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE) (pp. 62-68). IEEE.

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. Computers & Security, 68, 160-196.

Bailey, J. L., Mitchell, R. B., & Jensen, B. K. (2008). Analysis of student vulnerabili-ties to phishing. AMCIS 2008 Proceedings, 271.

Baumeister, R. F., & Leary, M. R. (1997). Writing narrative literature reviews. Review of general psychology, 1(3), 311-320.

Beaudry, A., & Pinsonneault, A. (2010). The other side of acceptance: Studying the direct and indirect effects of emotions on information technology use. MIS quarterly, 689-710.

Bissette, H. (2020). 'The threat of Covid-19 phishing attacks'. TheBusinessDesk. Retrieved January 31st 2021 from www.thebusinessdesk.com/yorkshire/news/2058462-the-threat-of-covid-19-phishing-attacks,

Bloom, N., Davis, S. J., & Zhestkova, Y. (2020). Covid-19 shifted patent applications toward technologies that support working from home. University of Chicago, Becker Friedman Institute for Economics Working Paper, (2020-133).

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77-101.

Braun, V., & Clarke, V. (2012). Thematic analysis.

Bree, R. T., & Gallagher, G. (2016). Using Microsoft Excel to code and thematically analyse qualitative data: a simple, cost-effective approach. All Ireland Journal of Higher Education, 8(2).

Brown, S. A., Fuller, R. M., & Vician, C. (2004). Who's afraid of the virtual world? Anxiety and computer-mediated communication. Journal of the Association for Information Systems, 5(2), 2.

Brynjolfsson, E., Horton, J. J., Ozimek, A., Rock, D., Sharma, G., & TuYe, H. Y. (2020). COVID-19 and remote work: an early look at US data (No. w27344). National Bureau of Economic Research.

Bullee, J. W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. Information & Computer Security.

Chen, Y., Zahedi, F. M., & Abbasi, A. (2011, May). Interface design elements for anti-phishing systems. In International Conference on Design Science Research in Information Systems (pp. 253-265). Springer, Berlin, Heidelberg.

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31.

Crouch, M., & McKenzie, H. (2006). The logic of small samples in interview-based qualitative research. Social science information, 45(4), 483-499.

Curran, K. (2020). Cyber security and the remote workforce. Computer Fraud & Security, 2020(6), 11-12.

Czaja, S. J., & Sharit, J. (1998). Age differences in attitudes toward computers. The Journals of Gerontology Series B: Psychological Sciences and Social Sciences, 53(5), P329-P340.

Drever, E. (1995). Using Semi-Structured Interviews in Small-Scale Research. A Teacher's Guide.

Engebretson, P. (2013). The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier.

Fafinski, S., Dutton, W. H., & Margetts, H. Z. (2010). Mapping and measuring cybercrime.

Finn, P., & Jakobsson, M. (2007). Designing ethical phishing experiments. IEEE Technology and Society Magazine, 26(1), 46-58.

F-Secure. (2021). What is phishing? Retrieved April 16th 2021 from: https://www.f-secure.com/en/home/articles/what-is-phishing

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. Field methods, 18(1), 59-82.

Gorling, S. (2006). The myth of user education. In Proceedings of the 16th Virus Bulletin International Conference.

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28(12), 3629-3654.

Hadnagy, C. (2010). Social engineering: The art of human hacking. John Wiley & Sons.

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

Hoxhunt. (2021). Retrieved January 20th 2021 from https://www.hoxhunt.com/gamified-phishing-training-platform/

Jakobsson, M., & Myers, S. (Eds.). (2006). Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. Journal of Management Information Systems, 34(2), 597-626.

Kang, A., Lee, J. D., Kang, W. M., Barolli, L., & Park, J. H. (2014). Security considerations for smart phone smishing attacks. In Advances in Computer Science and its Applications (pp. 467-473). Springer, Berlin, Heidelberg.

Kirlappos, I., & Sasse, M. A. (2011). Security education against phishing: A modest proposal for a major rethink. IEEE Security & Privacy, 10(2), 24-32.

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. IEEE Communications Surveys & Tutorials, 15(4), 2091-2121.

Leonardi, P. M. (2020). COVID‐19 and the New Technologies of Organizing: Digital Exhaust, Digital Footprints, and Artificial Intelligence in the Wake of Remote Work. Journal of Management Studies.

Li, L., & Helenius, M. (2007). Usability evaluation of anti-phishing toolbars. Journal in Computer Virology, 3(2), 163-184.

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to spear-phishing emails: Effects of internet user demographics and email content. ACM Transactions on Computer-Human Interaction (TOCHI), 26(5), 1-28.

Lister, K. (2020). 'Work-At-Home After Covid-19 – Our Forecast'. Global Workplace Analytics. Retrieved December 7th 2020 from: https://globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. Information Resources Management Journal (IRMJ), 24(3), 1-8.

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. All Ireland Journal of Higher Education, 9(3).

Malecki, F. (2020). Overcoming the security risks of remote working. Computer Fraud & Security, 2020(7), 10-12.

Mason, M. (2010, August). Sample size and saturation in PhD studies using qualitative interviews. In Forum qualitative Sozialforschung/Forum: qualitative social research (Vol. 11, No. 3).

McAfee. (2018). Economic Impact of Cybercrime - No Slowing Down. Retrieved April 12th 2021 from https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impactcybercrime.pdf

McAfee. (2021a). 2021 Threat Predictions Report. Retrieved April 16th 2021 from: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/2021-threat-predictions-report/

McAfee. (2021b). Phishing Email Examples: How to Recognize a Phishing Email. Retrieved April 16th 2021 from https://www.mcafee.com/blogs/consumer/phishing-email-examples-how-to-recognize-a-phishing-email/

Mokhtarian, P. L. (1991). Defining telecommuting.

National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cyber security and Infrastructure Security Agency (CISA). (2020). Advisory: Covid-19 exploited by malicious cyber actors. Retrieved December 7th 2020 from www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory

Newcomer, K. E., Hatry, H. P., & Wholey, J. S. (2015). Conducting semi-structured interviews. Handbook of practical program evaluation, 492.

Nilles, J. (1975). Telecommunications and organizational decentralization. IEEE Transactions on Communications, 23(10), 1142-1147.

O2 The Blue. (2020). 'A flexible future: Brits expected to call time on office life after lockdown'. Retrieved December 7th 2020 from: https://news.o2.co.uk/press-release/a-flexible-future-brits-expected-to-call-time-on-office-life-after-lockdown/ (6 May 2020)

Oest, A., Zhang, P., Wardman, B., Nunes, E., Burgis, J., Zand, A., ... & Ahn, G. J. (2020). Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In 29th {USENIX} Security Symposium ({USENIX} Security 20) (pp. 361-377).

Office for National Statistics (Great Britain)(ONS). (2020). Coronavirus and homeworking in the UK labour market: 2019.

Olson, M. H. (1983). Remote office work: changing work patterns in space and time. Communications of the ACM, 26(3), 182-187.

Orlikowski, W. J., & Barley, S. R. (2001). Technology and institutions: What can research on information technology and research on organizations learn from each other?. MIS quarterly, 25(2), 145-165.

Ozimek, Adam. (2019). "Overboard on Offshore Fears", Retrieved May 5th 2021 from: https://www.upwork.com/press/economics/report-overboard-on-offshore-fears/

Ozimek, A. (2020). The Future of Remote Work. Available at SSRN 3638597.

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

Raconteur. (2020). Retrieved May 5th 2021 from: https://www.raconteur.net/technology/cybersecurity/covid-19-cybersecurity/

Ragan, S., (& Staff Writer). (2013). Social engineering: study finds Americans willingly open malicious emails. Retrieved February 21st 2021 from http://www.csoonline.com/article/2133877/social-engineering/social-engineering--study-findsamericans-willingly-open-malicious-emails.html.

Rekouche, K. (2011). Early phishing. arXiv preprint arXiv:1106.4692.

Sarginson, N. (2020). Securing your remote workforce against new phishing attacks. Computer Fraud & Security, 2020(9), 9-12.

Steer, J. (2017). Defending against spear-phishing. Computer Fraud & Security, 2017(8), 18-20.

Trzupek, B. (2020). PKI is key to securing a post-Covid remote workforce. Computer Fraud & Security, 2020(10), 11-13.

Wetzel, R. (2005). Tackling phishing. Business Communications Review, 35(2), 46-49.

Williams, E. J., & Polage, D. (2019). How persuasive is phishing email? The role of authentic design, influence and current events in email judgements. Behaviour & Information Technology, 38(2), 184-197.

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. Journal of the Association for Information Systems, 16(6), 2.

APPENDIX 1: THE INTERVIEW STRUCTURE

Background information:

- How old are you?
- What is the industry you work in?
- How long has the employment lasted?
- In general, how much work experience do you have in this industry?
- How often do you work remotely?
- Have you switched mainly to remote work in March 2020 or later? (This question can be omitted if all interviewees are mainly working remotely)
- Have you worked remotely before March 2020?

Questions:

- Describe in your own words what kind of security training you have received in your company.
- Describe in your own words what kind of security threats you have experienced in your work.
- Has your company adopted new technologies due to the increase in remote work or significantly increased the use of certain technologies? What technologies?
- Have new technologies caused you problems? Which and in what way?
- Have you needed IT support while working remotely?
    - Have you received the support fast enough?
- Describe phishing in your own words.
    - Phishing seeks to exploit human vulnerabilities in the system. A typical attack method is to send an e-mail that contains a malicious file or a request to disclose sensitive (corporate or individual) information. Attacks can also be carried out through calls or text messages or on websites.
- Have you noticed a change in the number or quality of phishing attacks during your work? Describe possible changes.
- When a suspicious message has arrived, have you identified it immediately or been suspicious immediately?
- How often do you receive notifications related to scam messages?
    - If there is a notification, does it reach you before you open emails?
    - Do you feel it is a good practice to first ask co-workers if they have received such a message if you have received a suspicious message?
- Related to the above, do you feel there are any commonalities between the availability of new technologies, IT support and phishing attacks?
- Did you have any other thoughts on the topic?

APPENDIX 2: HAASTATTELURUNKO

Taustatietoja

- Minkä ikäinen olet?
- Mikä on ala, jolla työskentelet?
- Kauanko työsuhde on kestänyt?
- Paljonko sinulla on kaiken kaikkiaan kyseisen alan työkokemusta?
- Kuinka usein työskentelet etänä?
- Oletko siirtynyt pääasiallisesti etätöihin maaliskuussa 2020 tai myöhemmin? (Tämän kysymyksen voi jättää pois, jos kaikki haastateltavat ovat pääasiallisesti etätyössä)
- Oletko ennen maaliskuuta 2020 työskennellyt etänä?

Varsinaiset kysymykset

- Kuvaile omin sanoin, millaista tietoturvakoulutusta olet yrityksessäsi saanut.
- Kuvaile omin sanoin, millaisia tietoturvauhkia olet työssäsi kokenut.
- Onko yrityksesi ottanut uusia teknologioita käyttöön etätyön lisääntymisen johdosta tai lisännyt jonkin teknologian käyttöä huomattavasti? Mitä teknologioita?
- Ovatko uudet teknologiat aiheuttaneet sinulle ongelmia? Mitkä ja millä tavalla?
- Oletko etätyössä tarvinnut IT-tuen apua?
    - Oletko saanut yhteyden IT-tukeen riittävän nopeasti?
- Kuvaile omin sanoin phishing/tietojenkalastelu.
    - Phishingissä pyritään hyödyntämään ihmisestä johtuvia järjestelmän haavoittuvuuksia. Tyypillinen hyökkäystapa on lähettää sähköposti joka sisältää haitallisen tiedoston tai pyynnön luovuttaa arkaluontoisia (yrityksen tai yksityishenkilön) tietoja. Hyökkäyksiä voidaan suorittaa myös puhelujen tai tekstiviestien välityksellä tai verkkosivuilla.
- Oletko huomannut muutosta phishing-hyökkäysten määrässä tai laadussa työssäoloaikanasi? Kuvaile mahdollisia muutoksia.
- Kun epäilyttävä viesti on tullut, oletko tunnistanut sen samantien tai ollut epäileväinen heti?
- Tuleeko kuinka usein tiedotteita että on ollut huijausviestejä?
    - Jos tulee tiedote, niin saavuttaako se sinut ennen kuin menet avaamaan sähköposteja?

  - Koetko että on toimiva käytäntö ensimmäiseksi kysyä työkavereilta, onko heille tullut tällaista viestiä, mikäli sinulle on tullut epäilyttävä viesti?
- Edelliseen liittyen, onko mitään yhtymäkohtia uusien teknologioiden ja it-tuen saavutettavuuden ja phishing-hyökkäysten välille?
- Heräsikö mitään muita ajatuksia aiheeseen liittyen?