Master thesis project report

Navigating the Phishing Landscape: A Novel Stage Model Unveiling the Journey of Individuals Exposed to Phishing Attempts

FILIP ZEITZ SCHOU GRØTTERUD
KRISTIAN BJURHOLT REIN

SUPERVISOR
Wael Soliman

University of Agder, 2023
Faculty of Engineering and Science
Department of Engineering and Sciences

Obligatorisk gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

1.	Vi erklærer herved at vår besvarelse er vårt eget arbeid, og at vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen.	**Ja**
2.	**Vi erklærer videre at denne besvarelsen:** • Ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands. • Ikke refererer til andres arbeid uten at det er oppgitt. • Ikke refererer til eget tidligere arbeid uten at det er oppgitt. • Har alle referansene oppgitt i litteraturlisten. • Ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse.	**Ja**
3.	Vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§ 31.	**Ja**
4.	Vi er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert.	**Ja**
5.	Vi er kjent med at Universitetet i Agder vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk.	**Ja**
6.	Vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider.	**Ja**
7.	Vi har i flertall blitt enige om at innsatsen innad i gruppen er merkbart forskjellig og ønsker dermed å vurderes individuelt. Ordinært vurderes alle deltakere i prosjektet samlet.	**Nei**

Publiseringsavtale

Fullmakt til elektronisk publisering av oppgaven Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).
Oppgaver som er unntatt offentlighet eller taushetsbelagt/konfidensiell vil ikke bli publisert.

Vi gir herved Universitetet i Agder en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering:	**Ja**
Er oppgaven båndlagt (konfidensiell)?	**Nei**
Er oppgaven unntatt offentlighet?	**Nei**

Acknowledgements

This endeavor would not have been possible without the invaluable feedback from our thesis advisor Associate Professor Wael Soliman of the Department of Information Systems at the University of Agder. Our biweekly meetings have proven instrumental in maintaining a steady and efficient pace toward the completion of our thesis report.

We are also thankful to the anonymous practitioners who generously dedicated their valuable time and actively contributed to providing us with empirical evidence, thereby bolstering our data collection efforts.

Finally, we would like to express our deep appreciation for the unwavering support of our parents, friends, and significant other. Their belief in us has been a constant source of encouragement, sustaining our spirits and motivation throughout our years of study and during the process of researching and writing this thesis.

Kristiansand,
June 2nd, 2023

Filip Zeitz Schou Grøtterud	Rein
Filip Zeitz Schou Grøtterud	Kristian Bjurholt Rein

Abstract

The focus of this master thesis is to understand the process and stages individuals go through when exposed to a phishing attack. To achieve this objective, we will closely examine the responses of individuals throughout the phishing process and establish connections between their cognitive processes and actions, drawing upon relevant literature. By integrating these insights, we will construct a holistic phishing stage model. Consequently, our research question, "How can we identify and understand the stages involved in the phishing process?" will guide our investigation.

For this thesis, we conducted a qualitative study where we interviewed nine individuals from seven different IT consultant firms in Norway.

We utilized the theoretical framework to create a holistic phishing stage model. The findings lead to the creation of a phishing stage model consisting of a pre-stage and three main stages with constituent activities that explain the flow from stage to stage. The findings reveal that individuals rely on technical solutions in more ways than we initially thought. Warnings in the delivery stage of emails affects the potential victim in the later stages, especially when they explore the content of a phishing message. Ignoring phishing attempts were found to be prevalent in the younger interview candidates.

Interestingly those who reported phishing attempts were found to do so in two different ways, either officially or unofficially. The unofficial reporting consisted of altering coworkers through word of mouth or other communication channels. In contrast, official reporting was the way intended by company policies.

This study offers a valuable model that effectively explains the stages individuals go through during the phishing process. This research enhances our understanding of said phenomenon by shedding light on phishing attacks from the victim's standpoint. The insight gained from this thesis advances our understanding and offers valuable guidance for developing preventive measures, educational initiatives, training programs, and robust cybersecurity strategies. Furthermore, the model presented in this study serves as a valuable tool for identifying focal points in training efforts, thus enabling organizations to address vulnerabilities and effectively enhance their defenses against phishing attacks.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Since the 1990s, phishing has been used to attack individuals and companies, this attack which deceives the victim into doing or participating unwillingly in a malicious action is still as active today, and in 2022 it was a record year where 4.7 million phishing attacks were recorded by the Anti Phishing Work Group (APWG, 2023). Even though phishing is a more significant trend now than ever, many individuals still do not know what it is. In Proofpoint state of the phish report (proofpoint, 2023), it was found that one in three individuals could not define the concepts of malware, phishing, and ransomware, and only 56 percent of companies would train all employees in awareness training. Therefore, the options to defend against phishing are to utilize technical solutions or teach individuals to be aware of phishing.

In order to know how to help individuals protect against phishing, there is a need to understand how they react to phishing. This thesis aims to examine the phishing process holistically and develop a comprehensive phishing stage model that illuminates the stages involved in victimizing individuals through phishing attacks. Consequently, our research question is as follows: How can we identify and understand the stages involved in the phishing process?

Several models have been developed to shed light on the process involved in phishing attacks. The Phishing Funnel Model (PFM) proposed by Abbasi et al. (2021), The Life Cycle of Anti-Phishing by Khonji et al. (2013), and The Life Cycle of Phishing by Shaikh et al. (2016) are three such models. While these models provide valuable insights, they focus on specific aspects of the process and do not look at it holistically. For example, the PFM outlines the stages individuals take after entering a spoofed site without addressing the steps leading up to their entry. The life cycle of anti-phishing emphasizes the actions and countermeasures for detecting phishing rather than delving into the consequences when individuals fall prey to phishing attempts.

As a result, there remains a gap in understanding the complete sequence of events, which necessitates further research. Thus, a holistic phishing stage model is needed to explain the phishing process. This could be used both as a learning tool and also as a tool to understand how phishing harms companies. This understanding is vital in creating a healthy security culture that can reduce the harm phishing has and help individuals become better at detecting phishing.

1.1 The objective of the thesis

The objective of this thesis is, first and foremost, to understand the process, i.e., stages individuals go through when they are being phished, and to accomplish this, we will use a qualitative approach backed up by data from our literature review. We will interview employees from seven companies in the IT sector and attempt to understand their knowledge about phishing and their phishing experience to develop a holistic stage model that answers how individuals are phished.

The model's foundation will be inspired by the already existing predictive model, The Phishing Funnel model(PFM) made by Abbasi et al. (2021). However, we have seen that this model only covers the later stages of phishing. The model excels at predicting but can also be used to explain the later stages of the phishing process in which an individual has already have entered the spoofed site. Therefore we will use this data to describe the later stages in the model, While our research design aims to cover the early stages before an individual enters the spoofed site.

1.2 Research approach

This study uses a qualitative research approach to examine and understand how individuals get phished and the stages they go through in the phishing process. The technique used to gather data for this research was done through semi-structured interviews and research articles from various reputable journals. Our study began with a systematic literature review of forty articles. This literature review was conducted to develop an understanding of the concepts and phenomenon of phishing attacks from the victim's perspective. We chose to conduct the interviews using a qualitative approach since it aims to extract comprehensive information. Thus, it is especially valuable when studying social processes and the how of various events. Between April and May 2023, we conducted nine interviews which lasted between twenty to thirty minutes each, with IT consultants from seven different IT consultant firms in Norway. The first set of questions established the interviewee's role, technical abilities, and views on trust and risk involved with online engagement. The second set of questions in the interview focused on phishing and the phishing process. Here we established the interviewee's knowledge of phishing as well as diving into how they handle phishing attempts and their thought process along the way. Conducting the systematic literature review and the semi-structured interviews provided us with a theoretical foundation and empirical findings that allowed us to answer the research questions.

1.3 Thesis overview

Chapter 1 - Introduction provides an overview of the problem statement and the research question and provides the motivation for conducting this research.

Chapter 2 - Background and related work discusses the literature review process and the background and related research that create this study's foundation. This chapter also introduces the theoretical framework that informed our preliminary phishing stage model.

Chapter 3 - Research approach establishes why the chosen research approach and its premise is suitable for this study. This chapter will also present our research design, how we collected and analyzed the data, and the choice's limitations. Ethical considerations are also presented.

Chapter 4 - Findings presents the phishing stage model informed by the literature review and the findings collected from the interviews. The findings will be presented following the layout of the stage model.

Chapter 5 - Discussion/summary of findings is where we discuss our findings in relation to the findings from the literature review and the practical implications our findings have. Some directions for future research are also presented.

Chapter 6 - Conclusion provides a conclusion to the thesis and a reflection on the limitations of the thesis.

Chapter 2

Background and related work

This section will discuss the literature review process, providing an overview of the existing research on the topic and the methods used to conduct the review, including the databases and search terms used to identify relevant studies. The screening process will also be described, including the criteria used to evaluate the quality and relevance of the studies included in the review. This will be followed by a discussion and presentation of the background work from the literature review that forms the basis for our theory, highlighting the essential findings and their implications for the research. This will give a clear and comprehensive understanding of the current state of knowledge in the field and the areas where further research is needed. The section will conclude by describing the theoretical framework that our research is built upon. We will discuss the differences between variance and process approach to make an informed decision about what is best suited to our case. Ultimately we will present a preliminary phishing stage model informed by the systematic literature review.

2.1 Literature review

A systematic literature review (SLR) is critical to academic research. It allows us to review literature that is relevant to our thesis systematically. Webster and Watson (2002) states, *"A review of prior, relevant literature is an essential feature of any academic project. An effective review creates a firm foundation for advancing knowledge.”*. This statement tells us that by looking at past research, one can find gaps that have arisen and discover new paths of knowledge to explore.

"Most research starts with a literature review of some sort. However, unless a literature review is thorough and fair, it is of little scientific value. This is the main rationale for undertaking systematic reviews." (Kitchenham and Charters, 2007, p. 3). Additionally, our motivation for conducting an SLR is to better understand The Phishing Funnel model (PFM) by Abbasi et al. (2021) and the phishing process.

2.1.1 Method

For our SLR, we have chosen to follow Xiao and Watson (2019) model based on Kitchenham and Charters (2007) guidelines. Xiao and Watson (2019) process of systematic literature review consists of 8 steps: Formulate the problem, develop and validate the review protocol, search the literature, screen for inclusion, assess quality, extract data, analyze and synthesize data, and report findings. The model represents the steps we are taking when conducting our SLR as it provides a step-by-step approach that emphasizes the importance of straightforward research questions, explicit and transparent methods for searching, appraising, and synthesizing literature, and ethical considerations. By following the model's guidelines, we can ensure a comprehensive and valid review process that can provide valuable insights into the existing research on a specific topic.

2.1.2 SLR Criteria

Criteria had to be set in order to ensure the articles included were related and relevant to our research question. The criteria used in our SLR are shown below in table 2.1

Inclusion criteria	**Exclusion criteria**
Articles relevant to our research topic	Book or conference proceeding(not included ICIS, ECIS, or HICSS)
Studies that specifically focus on the topic of phishing and how individuals identify and respond to phishing attempts should be included in the review.	Studies that do not provide quantitative or qualitative data, as they may not be able to support the research findings
Peer-review studies	Not published in peer-reviewed journals
	Don't have a clear research question or methodology
	Outdated studies and not relevant to the current state of technology

Table 2.1: SLR criteria

2.1.3 Search process

In an SLR, we also have to systematically search for literature to find material for our review. When doing so, there are "three major sources to find literature: (1) electronic databases; (2) backward searching; and (3) forward searching." (Xiao and Watson, 2019, p. 103). "Because no database includes the complete set of published materials, a systematic search for literature should draw from multiple databases." (Xiao and Watson, 2019, p. 103). Thus in our search process, we used multiple electronic databases such as Web of Science, IEEE Xplore, and Google Scholar. In order to find relevant articles, we made a list of search words presented in table 2.2. These search words were combined using operators such as "Cybersecurity awareness" and "Phishing susceptibility".

The relevant literature was stored in an Excel sheet that provided an overview of the article's data. These articles were then used to conduct a backward search to identify relevant work cited by the article. We also conducted a forward search to identify articles that had since cited the stored articles (Xiao and Watson, 2019). We noticed that several articles identified sent us in a loop to other relevant articles already identified and stored in the Excel sheet. This gave us a rough estimate that we had identified a majority of the relevant articles concerning our thesis.

Search term	**Synonym/Specified term**
Cybersecurity	- Cybersecurity awareness - Cybersecurity behavior - Cybersecurity susceptibility factors - Cybersecurity susceptibility model - Human factors in cybersecurity
Phishing	- Social engineering - Phishing campaign - Phishing website - Spoofed site - Phishing process - Phishing model - Identify phishing - Phishing susceptibility - Phishing victimization - Anti-phishing
Awareness	- Cybersecurity awareness - Phishing awareness - Awareness training
Online deception	- Online deception and persuasion - Online deception and trust - Deception detection
Phishing funnel model	- PFM
Stage model	

Table 2.2: Keywords

2.1.4 Screening

After compiling a list of articles during the search process, we must determine whether each article should be included for data extraction and analysis (Xiao and Watson, 2019). This was determined by a screening process where we reviewed each article and examined them according to the established criteria. In order to visualize our screening process, we followed the PRISMA reporting standard for SLRs. The PRISMA flow diagram can be seen in figure 2.1.

The screening process started by identifying relevant articles by using the mentioned keywords in searches on databases such as Web of Science and IEEE Xplore and applying the set criteria. A supplementary search was made using Google Scholar. After duplicates were removed, we identified 104 articles. These articles were then screened by reviewing the title. Articles with irrelevant titles were excluded. Thus 76 articles remained and went on to be screened by reading the abstract and reviewing the relevancy. After the abstract screening, 59 articles remained and went on to be reviewed by reading the complete text, i.e., reviewing the most representative information from each article by reading the introduction, findings, results, conclusions, summaries, and possibly other relevant chapters. After this last step, we were left with 40 eligible articles. That went on to be synthesized by coding each article in Nvivo.

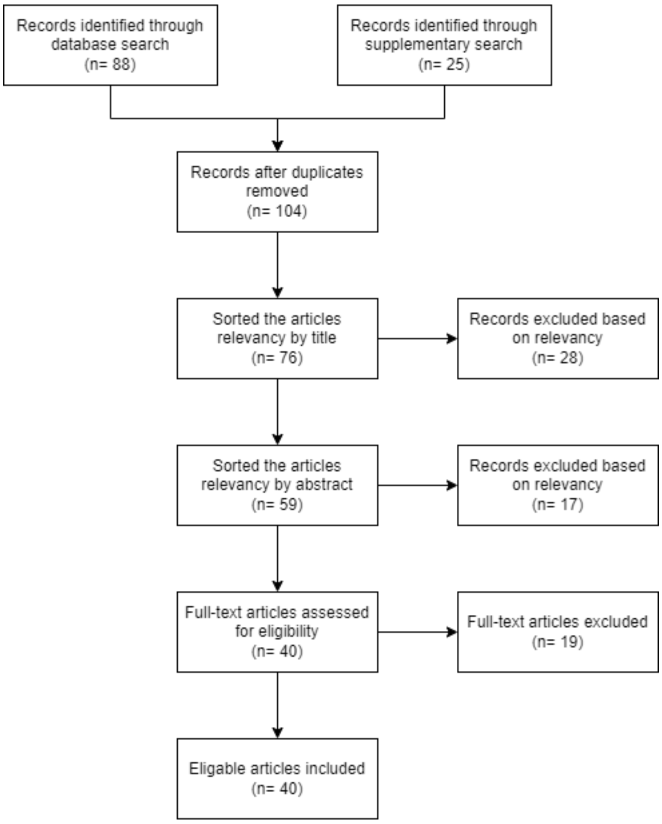

Records identified through database search (n= 88)
Records identified through supplementary search (n= 25)
Records after duplicates removed (n= 104)
Sorted the articles relevancy by title (n= 76)
Records excluded based on relevancy (n= 28)
Sorted the articles relevancy by abstract (n= 59)
Records excluded based on relevancy (n= 17)
Full-text articles assessed for eligibility (n= 40)
Full-text articles excluded (n= 19)
Eligable articles included (n= 40)

Figure 2.1: Systematic literature review

2.2 Phishing

Anti-Phishing Work Group (APWG, a) reported in their 2022 first-quarter report that, for the first time, their number of phishing attacks had reached over 1 million in a quarter. This trend has continued throughout 2022, and in their third-quarter report (APWG, b), they reported that the number had increased to 1,2 million quarterly phishing attacks, but how do we define phishing in 2023? Our definition of phishing will be constructed from a collection of definitions from multiple researchers. These definitions are presented in table 2.3.

From these definitions, we see phishing as an attack with the goal of deceiving one or more receptors through a communication channel into doing or participating unwillingly in a malicious action. Most definitions from table 2.3 define the communication channel as email but with the phishing technique SMiShing which exploits the technical abilities that have come with modern messaging applications (Yeboah-Boateng and Amanor, 2014). We, therefore, see that there is a need for a definition which, in a broader sense like Rader and Rahman (2015) is needed to encapture the attack vector phishing can have over multiple communication channels in 2023.

There are multiple techniques of phishing mentioned in the definitions from table 2.3. Williams et al. (2018) and Wang et al. (2012) mention spear-phishing, which is a targeted variant of phishing. In addition to these definitions Yeboah-Boateng and Amanor (2014) mentions SMiShing. In their paper, they also mention Vishing which is phishing utilizing Voice over Internet Protocol (VoIP) to social engineer their victim to give away their credentials. These techniques have variants that all change the attack vector in which phishing can happen. Spear-phishing, which Williams et al. (2018) and Wang et al. (2012) mention, utilizes information to get the victim's trust. The attacker will study their victim and learn the information they can exploit before launching an attack. The attack will then utilize this

Definition	Author
Email-based deception where a perpetrator(phisher) camouflages emails to appear as a legitimate request for personal and sensitive information is known as phishing.	(Wang et al., 2012, Page 345)
One means by which this can be achieved is via targeted, fraudulent emails, which aim to persuade employees to click on malicious links, download malicious attachments, or transfer organizational funds or other sensitive information.	(Williams et al., 2018, Page 1)
These attacks are designed to trick users into thinking an e-mail or website is legitimate and to convince them to divulge usernames and passwords or to inadvertently install malware by clicking on malicious links or attachments.	(Canfield et al., 2016, Page 1158)
Phishing is a social engineering technique that is used to bypass technical controls implemented to mitigate security risks in information systems. People are the weakest link in any security program. Phishing capitalizes on this weakness and exploits human nature in order to gain access to a system or to defraud a person of their assets	(Rader and Rahman, 2015, Page 23)

Table 2.3: Phishing definitions

information to have a higher likelihood that the victim will follow through on the phishing attack. Even though there are multiple techniques for phishing, the attacker usually has the same goal.

From an attacker's perspective, the goal with phishing can be multiple motives but usually falls into a financial motive in which the attacker does this for capital gain. However, they could also hide their identity by using stolen identities for criminal purposes or to gain recognition from their peers or communities (Khonji et al., 2013).

2.2.1 Life-cycle of phishing

Phishing has multiple life cycles depending on the perspective of the individuals conducting the phishing campaign. This perspective depends on the motives of how they would look at phishing.

Anti-phishing perspective

Khonji et al. (2013) describes in their literature review the view individuals could have when looking at phishing from an anti-phishing perspective. First, a phishing campaign will begin, and if not detected, the anti-phishing team has to learn from it, or it will continue in a negative loop until detected. The campaign can be detected by user awareness, in which a potential victim is aware of a phishing attempt and reports the attack, or by software detection, in which technical solutions hinder the phishing attempt(Khonji et al., 2013). We will cover the technical solutions later in this chapter.

When an attack has been detected, the anti-phishing team has three options. First, they can apply offensive defense actions, which are software tools that will disrupt the phishing campaign, an example of this would be a tool that fills the phishing campaign with fake credentials so that the real potential credentials will be harder to identify. However, it is unknown how hard this approach makes for the attacker since they could set up a script that tests the credentials in an anonymous environment. The second option for the anti-phishing team is to go for a corrective approach in which they go after the service providers of the phishing campaign. They could do this as a phishing campaign containing multiple resources like websites, email services, social network services, and other IT services and by reporting the misuse of the service to the provider. The provider can then correct the misuse by attempting to remove the resources utilized (Khonji et al., 2013).

The third option is to go for a preventative approach. This option, however, can be a multiple of things as there are multiple prevention options. One of the options is to prevent individuals from becoming victims by educating them on the threat of phishing and having prevention software, making it harder for a phishing attempt to reach potential victims. Another option is to prevent attackers from starting campaigns by using lawsuits or legal action through law enforcement agencies. However, the prevention approach is often just seen as the first option, as the second option is more expensive and takes longer to respond to the threat (Khonji et al., 2013).

Attacker's perspective

The life cycle of phishing changes when we look at it from an attacker's perspective. Shaikh et al. (2016) describes in their paper the five stages that phishing goes through from an attacker's perspective. These stages are visualized in figure 2.2. Where the first stage is the planning and setup stage. Here the attacker identifies their potential targets and the scope of the attack. They will then set up the resources needed, such as websites, email services, and malicious software. The second stage is the phishing stage. This stage has the most activity from the attacker's perspective. They will deploy the attack toward the victim chosen and will usually send spoofed emails containing a factor of urgency (Burns et al., 2013)(Shaikh et al., 2016).

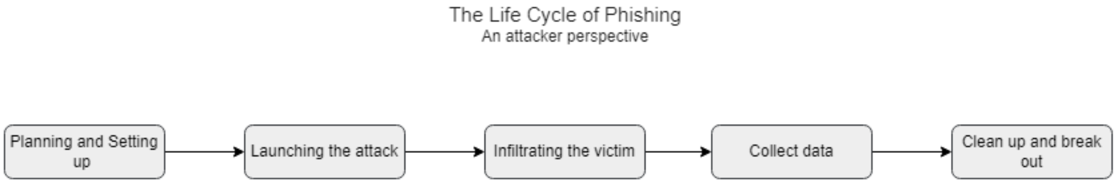


Figure 2.2: Our illustration of the life cycle of a phishing campaign from an attackers perspective (Shaikh et al., 2016)

This urgency can create the factor needed for stage three, the break-in/infiltration stage of phishing, where the victim has pressed the malicious link. They would then be either sent to a spoofed website or downloaded malicious software giving the attacker access. The software would then change access rights and configurations for remote access. After the initial infiltration stage, the attacker would be at stage four of data collection. This stage aims to collect data that can be used to either press the victim for financial gain or gain credentials that can be used for a loss further down the line. They get the data either from spoofed websites or by installing malware on the victim's device (Shaikh et al., 2016).

From an attacker's perspective, the fifth and last stage of the phishing life cycle is the break-out/ex-filtration stage. After the attacker has gained the data or done the harm they wanted, they will clean up the evidence and remove services that are no longer needed. Some attackers will then track the degree of success they had to refine their future attempts to trick people into falling for phishing (Shaikh et al., 2016).

Victim's perspective

Now that we have looked at phishing from the attacker's perspective, we can turn the tide and view it from the potential victim's perspective. Since we are to research how individuals get phished and what stages they go through in the process, synthesizing the literature that touches upon this is crucial. Abbasi et al. (2021); Abroshan et al. (2021); Burns et al. (2013) all have research phishing stages to some degree. What most other prior phishing studies have done is focus on a single decision or action, often whether or not someone considers a website legitimate or if they are willing to transact with a phishing website (Sheng et al., 2010; Dhamija et al., 2006). However, as Abbasi et al. (2021) mentioned falling prey to a phishing attack entails a sequence of interrelated decisions and actions, and modeling these sequences as a gestalt it would provide us with deeper insight into the phishing process.

Abbasi et al. (2021) created the phishing funnel model, which is a design artifact for predicting user susceptibility to phishing websites (Abbasi et al., 2021). PFM incorporates factors related to users, threats, and tools to predict users among the four stages of the phishing process. These stages are visit, browse, consider legitimate, and intend to transact, regardless of how a phishing website is entered. Abbasi et al. (2021) said that users are faced with the four stages mentioned and sequentially faced with four progressively dangerous decisions that ultimately determine users' susceptibility. PFM excels at predicting users' susceptibility. However, what is interesting in our case is that it explains or describes the different stages in the phishing process. Nonetheless, they only provide insight after a user has entered or visited a spoofed site.

Abroshan et al. (2021) argues that it is important to understand what type of behavior and attitudes can influence us to follow the path the attacker wants us to take in each step of the phishing process. The reasoning behind this argument is that many scammers follow a step-by-step approach to phishing. This process aims to gain trust and guide the victim toward the desired actions. This can be compared with the cyber kill chain developed by Lockheed Martin (LockheedMartin, 2023), but in this context, it is crucial to understand and defend against "the phishing kill chain". According to them, the phishing process consists of three steps: The first step is opening the phishing email. Here the email has circumvented technical barriers and ended up in a user's email inbox. The second step is clicking on a phishing link. This can be done by clicking a link or opening an email attachment. Clicking the link usually results in opening a phishing website where the attacker tries to extract sensitive information from the victim. The third and last step is to give information to the phisher by "submitting sensitive information, taking the requested action, or when the built-in malware is not detected/prevented by any endpoint security system (e.g. antivirus software, mobile security, so on) and the malware compromises the user's device (i.e. computer, mobile phone, tablet, etc.) or account (i.e. email account, company account, etc.)." (Abroshan et al., 2021)

Burns et al. (2013) examined how to promote protective behavior for IS end-users. They found that users progress through stages of preventive behavior. These stages range from a denial stage (Stage 0), an awareness stage (Stage 1), and a coping and planning stage (stage 2). From this, Burns et al. (2013) proposed a 3-stage research model called Security Action Stage Model (SASM). At stage 0 (Low Intender), individuals may exhibit risky behavior like clicking a link or opening an attachment in an email. The reason for them doing this is that their perception of being vulnerable to phishing is low. Regardless of training relevant to phishing, they think the probability of falling for a phishing attempt is extremely low. Those who reach stage 1 (Intender) have realized they are vulnerable to phishing attempts. It is in this stage that we begin to see behavioral changes. These changes could be to learn and become more attentive to leakage cues. Finally, in stage 2 (Actor), individuals take active steps to prevent future phishing attempts. These steps include the development of an action or coping plan in case they should become the victim of a phishing attack, as well as gathering knowledge and learning about phishing precautions.

2.2.2 Phishing susceptibility

Now that we understand what phishing is, we must understand how some people fall for phishing, and some seem more resilient. Several researchers have touched upon susceptibility to phishing in some way or form (Abbasi et al., 2021; Harrison et al., 2016; Martin et al., 2018; Moody et al., 2017; Sheng et al., 2010). Abbasi et al. (2021) defined phishing susceptibility as the extent to which users interact with the phishing attack. Most commonly, it is assumed that phishing attack refers to emails. However, susceptibility to phishing is not specific to email and explains the susceptibility of an individual regardless of the delivery method of the phishing attack. Other researchers attempted to clarify what determines susceptibility to phishing and, in the process, explained phishing susceptibility as "*a function of being immersed in the email without sufficient consideration of its meaning and viability in a larger context.*"(Harrison et al., 2016, p. 277). Phishing susceptibility can also be looked at as the likelihood of an individual responding to the attack and the response time Martin et al. (2018).

Since the goal of a phishing attack is to trick the victim, the victim's susceptibility plays a crucial part for the attacker and businesses since having employees with lower susceptibility lower the chances of a breach (Alder, 2022). Thus multiple researchers have examined what factors can impact an individual's susceptibility. Moody et al. (2017) conducted a literature review to explain why certain individuals are susceptible to phishing attacks. They found that susceptibility can be considered from two primary angles. The first angle consists of the attributes of the recipient of the email, i.e., the attack target or potential victim. In contrast, the second angle is the attributes of the phishing attack, often the attributes of the email.

The first angle has been studied from a social engineering perspective by Workman (2008). Among the attributes mentioned in the literature, we found an emphasis on knowledge and prior experience Abbasi et al. (2021); Burns et al. (2013); Harrison et al. (2016); Moody et al. (2017); Qabajeh et al. (2018); Vishwanath et al. (2011). This knowledge refers to an individual's security knowledge, awareness of phishing, and technical abilities or expertise. Prior experience refers to general web experience and usage as well as past encounters or losses from phishing. Demographics are also a factor impacting susceptibility. Age (Sheng et al., 2010; Vishwanath et al., 2018; Abbasi et al., 2021; Das et al., 2022; Moody et al., 2017), gender (Abbasi et al., 2021; Abroshan et al., 2021; Vishwanath et al., 2011; Moody et al., 2017) and education (Abbasi et al., 2021) was found to impact susceptibility. Younger people tend to engage more in online activities, and the age group 18-25 are most likely to fall for phishing (Sheng et al., 2010). When it comes to gender, researchers have been split on whether it has an impact or not. Sheng et al. (2010) found that the difference in susceptibility between the genders appears to be caused by a difference in technical training and technical knowledge, thus strengthening the argument for why knowledge is an important factor. Self-efficacy, i.e., the ability to complete recommended actions and sequentially computer self-efficacy, was also found to impact susceptibility Abbasi et al. (2021); Vishwanath et al. (2011).

The second angle consists of the attributes of the phishing message. Wright et al. (2014) tested several techniques to influence individuals through the content of an email message.

> *They found that a number of techniques were successful in significantly predicting user compliance. These included liking the perceived sender, reciprocity (implying that the sender has done things for the recipient), social proof (purporting that a given behavior is the correct social behavior), consistency (implying that a given behavior is consistent with past behaviors), authority (the message indicates that it is from someone in authority), and scarcity (making an opportunity appear less available).* (Moody et al., 2017, p. 566)

Other attributes of the phishing message are called leakage cues, which we will return to later in this section.

Ultimately, individuals' susceptibility to a phishing attempt lies in their ability to recognize and resist such malicious tactics. As mentioned, several factors influence this likelihood, i.e., susceptibility. However, in essence, the differences among individuals when it comes to processing, in terms of user's attention and elaboration of the phishing messages, ultimately lead to differences in susceptibility to phishing (Harrison et al., 2016). Vishwanath et al. (2011) explained the same context slightly differently. They discovered that individuals get phished for two main reasons. First, they do not adequately process the information but instead rely on simple cues that can potentially increase their susceptibility. The second reason, which strengthens the first, is that habitual patterns of media use tend to trigger automatic responses to relevant-looking emails. Thus, how we process information can majorly impact individuals' susceptibility to phishing. We will come back to this at a later point in this chapter.

2.3 Technical solutions

The technical solution is all the preventative software used to prevent phishing from reaching a potential victim. This software can be blacklist, heuristic, visual, or machine learning software (Khonji et al., 2013). The technical solutions also have a solution after the initial detection of phishing in which the software works more to hide. This section goes deeper into how the different preventative software works and how they're used.

2.3.1 Blacklists

Blacklists are lists filled with previously detected phishing URLs, IP addresses, or keywords. They are frequently updated to remain efficient but cannot protect against zero-day phishing attempts as they need to have prior knowledge about the phishing attackers' URL, IP, or specific keywords for that attempt to block it. A company that looks at blacklists can implement the opposite version, a white list. The company will accept only specific URLs or IP addresses in a white list instead of blocking them. (Khonji et al., 2013)

Some examples of a blacklist are the Google safe browsing API which validates a client's given URL towards a constantly updated Google database. A DNS-Based blacklist utilizes the DNS standard to check for blacklisted URLs. However, if the DNS server is large and not optimized for handling greater amounts of DNS A or TXT Resource Records, it could strain the performance and resources of the DNS server. There is also predictive blacklist software like PhishNet which will try to solve the problem in which a blacklist needs an exact URL or keyword to activate by creating variants of the Top-level domains and looking for similarities in the directory of the sites. Doing this heuristically can remove multiple phishing attempts by looking for leakage cues (Khonji et al., 2013; Butavicius et al., 2022).

2.3.2 Heuristic

In a heuristic software approach toward phishing detection, you could use software installed on the client or server side. The software would look at different payloads using different algorithms. These protocols could be HTML, SMTP, or any regularly used protocols. In addition, the algorithms would look after any leakage cues for phishing. This means that the software could detect a zero-hour phishing attack. However, this approach can lead to legitimate content being classified as phishing. Spoof guard is an example of heuristic phishing detection software. It is a web-browser plugin developed by Stanford University which detects HTTPS-based phishing attempts by weighing certain anomalies found in the HTML (Khonji et al., 2013).

2.3.3 Visual

Visual phishing detection software attempts to identify phishing from their visual appearance instead of analyzing the source code or network-level information. Different from the other technological solution, visual software looks at the site's appearance. This can benefit in detecting phishing attempts where the HTML is designed to trick the heuristic and predictive approach. The visual approach work in many different ways. One example is taking snapshots of the suspected site and converting the RGB colors into a grayscale. The software will then look for key features or salient points using the Harris-Laplace algorithm to calculate the total number of positive to negative pixels that differ. This, however, can cause a higher amount of false positives (Khonji et al., 2013).

2.3.4 Machine learning

Machine learning software, in this case, would be document classification and clustering problems in which models are constructed by taking advantage of machine learning and clustering algorithms like k-Nearest Neighbors(k-NN), C4.5, Support Vector machines, k-means and Density-Based Spatial Clustering of Applications with Noise(DBSCAN). These algorithms will create a classification system through training or decision-making to detect whether the content is a phishing attempt. Although they differ in how they conclude, k-NN will, through training, create multi-dimensional vectors where the given vector represents a particular feature. C4.5 constructs a decision tree that should be unspecific enough to correctly classify unseen instances (Khonji et al., 2013).

There are suggested solutions for automatically detecting phishing targets from phishing web pages by looking at the phishing site and the suspect page and finding its most similar page with a different domain name. An example could be if EBay.com was found to be the site with the most resemblance to the suspect site, then the suspect site would be assumed as phishing. This solution can also be made using parts of the other approaches, such as the visual approach (Khonji et al., 2013).

2.4 Non-technical solutions

In contrast to technical solutions, the literature also reveals non-technical solutions to combat phishing. At the forefront of this is awareness training. Several articles mention different methods of conducting this type of training and the importance of it (Kumaraguru et al., 2007, 2009; Miranda, 2018; Nguyen et al., 2023). We find rule-based training, embedded training, mindfulness, and over-learning among these different methods.

2.4.1 Rule-based training

The premise of rule-based training is that it teaches an individual how to apply a set of guidelines in the process of exploring a message. An example of such a guideline is never clicking on embedded links from unknown senders (Nguyen et al., 2023). In addition, rule-based training relies on identifying leakage cues, which we will return to later in this chapter. Rule-based training's goal is to teach individuals simple rules and cues to look out for that will aid individuals in exploring phishing emails and evaluating the legitimacy of emails.

2.4.2 Mindfulness

In the literature about mindfulness in the context of antiphishing training, mindfulness refers to the attention and awareness of an individual's experience in the present. It provides a better understanding of a situation and possible future implications of an individual's actions (Nguyen et al., 2023). To put this more in context, it tries to train individuals to focus on three key steps. The first step is to pause before clicking a link or responding to an email. The second is to reflect on what is being requested and the message's context and underlying motive. The third step is to verify from a third party if the email's legitimacy is in question (Nguyen et al., 2023). Interestingly they found that "*antiphishing training incorporating mindfulness techniques is more beneficial by helping individuals better discriminate between legitimate and phishing emails and become less susceptible to phishing attacks but not in terms of making individuals more cautious towards phishing*" (Nguyen et al., 2023, p. 22).

2.4.3 Over-learning

Over-learning can be seen as a supplementary type of training. It is defined as "*the deliberate overtraining of a task past a set criterion*" (Driskell et al., 1992, p. 615). It can be used as an aspect of rule-based training by overtraining rules. This type of training was valuable when paired with the mentioned rule-based training and mindfulness training, specifically when it came to increasing an individual's vigilance towards phishing (Nguyen et al., 2023).

2.5 Theory

The theory section of this study delves into several significant theories that illuminate the intricate processes of information processing, detection of leakage cues, deception theory, and the protection motivation theory. Understanding how we absorb and interpret information, identify leakage cues, analyze deceptive behaviors, and motivate ourselves to protect against potential threats are crucial. By examining these theoretical frameworks, we aim to shed light on the underlying mechanisms that shape our cognitive processes, decision-making, and responses to phishing messages.

2.5.1 Information processing

The literature related to phishing often mentions how individuals process the information in the phishing message, most commonly phishing emails. However, it could be transferred to other delivery methods. Information processing is interesting in the context of phishing since phishing victims are often forced to make quick decisions based on leakage cues found in the phishing message. Cues such as urgency may distort our ability to detect deception (Burns et al., 2013). We will come back to leakage cues later in this section. There has been extant research on phishing that has "*implicated users' cognitive processing as a key reason for individual victimization*" (Harrison et al., 2016, p. 266). In order to investigate individuals' cognitive processing, researchers have used two different dual-process models, which are the heuristic systematic model (HSM) (Vishwanath et al., 2018; Luo et al., 2013) and the elaboration likelihood model (ELM) (Harrison et al., 2016; Vishwanath et al., 2011). It is interesting to look at how individuals process information since "*a scammer might use human cognitive and behavioral attributes to design their tricks and to fool victims*" (Abroshan et al., 2021, p. 44928). Thus by understanding human cognitive and behavioral attributes related to information processing, we could get insight into the process an individual faces when being targeted by a phishing attempt.

In the first model, HSM, there is a distinction between two modes of information processing that individuals employ. These processing modes are systematic and heuristic processing. Heuristic processing takes advantage of factors embedded within or surrounding a message. These factors are called heuristic cues. This could be the message source, format, length, and subject. These factors are then used to assess the message's validity rapidly. This does not require many cognitive resources and is done quickly (Luo et al., 2013). While on the other hand, systematic processing carefully researches the message's information to judge its validity. Thus it requires more time and cognitive resources than heuristic processing. According to Luo et al. (2013), individuals tend to limit their time investment and cognitive resources if there is a lack of motivation or capability. Several factors may affect individuals to invest or not invest cognitive resources, such as perceived importance of the decision outcome, perceived risks, time and other pressures, skill level, and distractions (Luo et al., 2013). Vishwanath et al. (2018) explained HSM slightly differently:

> *At the upper end of the information-processing continuum is systematic processing, where individuals make judgments by carefully examining the quality of arguments within the persuasive context. At the other end is heuristic processing, which involves the use of simple decision rules or cognitive heuristics triggered by adjunct cues in the context to reach judgments. As mentioned in the previous section, habitual patterns of media use tend to trigger automatic responses. From a cognitive resource standpoint, systematic processing is effortful and requires the allocation of substantial information-processing resources, while heuristic processing is more economical and efficient.* (Vishwanath et al., 2018, p. 1150).

The second model, ELM, was initially created to explain how consumers respond to and process stimuli like persuasive advertising messages. Petty et al. (1986) found that consumers processed information in two different ways. The first is the central processing route, which is similar to systematic processing. It involves diligently considering the information by comparisons and prior experience (Harrison et al., 2016). The second is the peripheral processing route, which is similar to heuristic processing, where the consumer does not consider all the message elements but relies on simple cues in the persuasion context (Vishwanath et al., 2011).

Although ELM was made regarding persuasive advertising messages, it is applicable in the context of phishing since it provides a theoretical framework to help us understand the process of victimization through phishing. This is because it allows us to examine how attention to leakage cues can result in the victim either resisting or succumbing to the attack (Harrison et al., 2016). Similarly to HSM, the amount of mental focus or cognitive resources allocated to specific elements of the message determines what route is chosen when judging the validity of the phishing message. This choice between the two routes "*occurs when individuals make connections between these elements and prior knowledge and experience.*" (Harrison et al., 2016, 1470). Greater knowledge means fewer cognitive resources are required to trigger the central processing route.

Leakage cues

We have mentioned leakage cues several times, but what exactly are they? Leakage cues, also known as missing or phishing cues, are characteristics of deceptive communication that can identify it as such, despite the threat actor's effort to appear genuine (Butavicius et al., 2022). These cues can be features such as impersonal greetings, suspicious URLs with a deceptive name or IP address, unusual content based on the alleged sender and their subject, requests for urgent action, grammatical errors, and misspellings (Canfield et al., 2016). Parsons et al. (2016) concludes that phishing emails have, in general, more spelling mistakes and are less likely to be personalized, consistent, and have legitimate links and sender. Butavicius et al. (2022) states

> *These mechanical errors are often present not just in the email lures created by the attackers but also in the phishing websites linked in these emails* (Butavicius et al., 2022, p. 2).

This means that leakage cues are represented not only in the communication process of the phishing attack but also in the whole life cycle of phishing.

Butavicius et al. (2022) studied the effect of urgency and the use of leakage cues that could be used to discover phishing. They found that even though leakage cues were presented in the communication, it had little to no effect on the resistance towards phishing, but their study had an overall poor detection of phishing. This result is similar to other studies, as leakage cues and their effect have shown mixed results. Studies such as Canfield et al. (2016) have shown that individuals will have less susceptibility when they pay greater attention to leakage cues and have greater general paranoia.

However, studies such as Parsons et al. (2016) study on which leakage cues an individual uses to legitimize an email suggest that individuals often get influenced by cues that can not conclude towards a phishing attempt. The individuals in their experiment would often use visceral cues such as legal disclaimers, visual design, and positive consequences as cues. Butavicius et al. (2022) concludes that leakage cues do not influence an individual's resistance toward a phishing attack.

2.5.2 Deception Theory

Deception theory is explained using two theories by Vishwanath et al. (2011). The first theory is interpersonal deception theory(IDT), which argues that the key to identifying deception is the verbal and non-verbal leakage cues the deceiver displays through the process. In phishing, however, there is not necessarily an interpersonal interaction. Here, other communication through channels such as email or messaging applications can be used as the stimulus to detect phishing. The other theory used by Vishwanath et al. (2011) is the theory of deception which is similar to IDT but focuses more on the information processing involved in detecting deception.

The theory of deception states that individuals discover deception by noticing the inconsistency between the deceptive events and their prior experience. The theory is built around four stages in which the first stage is the activation stage, where an individual sees deceptive information and finds anomalies. From detecting the inconsistency, the individual moves to the second stage, where the individual generates a deception hypothesis based on their former knowledge to explain the anomalies. Following the creation of the hypothesis, the individual evaluates their hypothesis in the third stage by following the hypothesis compared to some criteria. The final stage is a global assessment stage, where the information gathered is formed into a single assessment of deceptiveness. This assessment is subjective and based on the individual's prior experience and knowledge (Vishwanath et al., 2011).

2.5.3 Signal detection theory

Signal detection theory (SDT) is a theoretical framework used when a situation has two classes of events to be discriminated against. The general assumption is that each decision the subject makes is based on the many characteristics of the event in question (Pastore and Scheirer, 1974). In phishing, it has been used to test an individual's performance on email classification tasks. Signal detection theory provides a better insight into the decision-making process behind phishing detection. The discrimination in this context would refer to an individual's ability to distinguish between a phishing email and a legit email (Butavicius et al., 2022).

2.5.4 Protection motivation theory

Protection motivation theory (PMT) is a theoretical framework used to understand how individuals decide to engage in behaviors involving risk or threat. According to PMT, individuals will engage in protective behavior if they perceive a threat and believe that the behavior will effectively reduce that threat and if they perceive themselves as capable of performing the behavior. This fear appeal is strongly related to ELM since a user is motivated to protective action when a message stimulates a fear response (Rogers, 1975; Johnston and Warkentin, 2010). In addition, PMT suggests that individuals are more likely to engage in protective behaviors if they have a high level of perceived vulnerability to the threat and believe that the potential consequences of not engaging in the behavior are severe. PMT also recognizes the importance of factors such as self-efficacy, perceived response efficacy, and perceived costs in shaping an individual's decision to engage in protective behavior (Moody et al., 2017).

Taking a look at prior research concerning trust and distrust, "*the majority of phishing and IS behavioral security research has relied upon the theoretical background of PMT, which proposes that fear appeals persuade individuals to protect themselves from threats.*" (Moody et al., 2017, p. 576). Since many cases of phishing emails rely on constructs indicated in PMT, i.e., fear appeals, it is imperative to have an understanding of what PMT is in order to get insight into individual thought processes during the phishing process and, subsequently, the stages in said process.

2.6 Theoretical framework

In order to build or create something, it usually helps to have a plan, scaffolding, or framework to follow. For this thesis, we have decided to use a theoretical framework as a scaffolding to build from. The literature shows that we know a great deal about phishing and how to predict the susceptibility of individuals as well as how far into the attack one is likely to venture (Abbasi et al., 2021; Harrison et al., 2016; Vishwanath et al., 2011; Burns et al., 2013; Abroshan et al., 2021). However, there is a gap in the literature since little is known about the process or the stages as a whole that individuals go through when being targeted by a phishing attack. This is where the theoretical framework comes in. Suppose we are to look at the logical structure of a theory. In that case, two contrasting approaches are often mentioned: the variance (i.e., static approach or stage-less theories) and the process (i.e., dynamic approach or stage theories) approach (Soliman and Tuunainen, 2022; Tsohou et al., 2020; Van de Ven and Engleman, 2004).

For the variance or stage-less approach, the phenomena of interest, its factors, explanations, or variables are expected to have an unchanged meaning and identity during the life cycle of the phenomena (Tsohou et al., 2020; Soliman and Tuunainen, 2022). If we look at the process or stage approach, it is needed when the same factors are assumed to be developing and changing throughout the lifespan of the phenomena Tsohou et al. (2020). In other words, "*the variance approach captures the continuous variation in development and change with powerful mathematical representations, whereas the process approach includes the role of human agency in change and development.*" (Van de Ven and Engleman, 2004, p. 356). As Soliman and Tuunainen (2022) put it, the variance perspective might be well suited to answer 'what' questions; however, the process perspective is more suited to answer 'how' questions. Following this reasoning, we will approach our RQ through the theoretical lens provided by the process approach or stage modeling. By doing so, we can create a foundation for the empirical part of our research since it allows us to set up the aforementioned scaffolding to further build from.

A requirement for a theory to be called a stage theory is that it has ordered stages, according to Tsohou et al. (2020). What this means is that stage theories consist of stages that are used to understand the development path of a phenomenon. In other words, how behavior changes or evolves. As Tsohou et al. (2020) put it, "*Stage theories suggest that development is linked to stages. Therefore, stage theory endeavours to explain the development path of a specific phenomenon by dividing the development into distinct stages*" (Tsohou et al., 2020, p. 8). Thus, every stage model has in common that it has two or more ordered stages with different elements that explain the behavior and movement between the stages of an individual (Tsohou et al., 2020; Weinstein et al., 1998). The usefulness of a stage lies in its ability to simplify and aid in comprehending a complex phenomenon, despite being a theoretical construct that does not exist in nature. The movement or progression through stages is not implied to be inevitable or irreversible. Because of the flexibility of human behavior, individuals do not need to spend a fixed amount of time in any stage (Weinstein et al., 1998). For example, one individual might spend more time than another deciding whether or not to click a suspicious link and venture into the next stage, while a third might not click the link at all.

2.6.1 Variance vs process approach

Since we have established our theoretical framework for the thesis, it could be interesting to identify the differences between a variance approach and a process approach, as well as what approach the different articles in our literature review have followed.

As previously mentioned, variance theories focus on the variation or differences among individuals or groups. It seeks to identify factors that cause these variations and often uses statistical analysis to quantify and measure these differences. While synthesizing the literature, several theories and models follow the variance approach (Butavicius et al., 2022; Moody et al., 2017). Variance approaches typically identify the effects of independent variables on the dependent variable, but they may not explain how or why these variables affect the outcome. Since our thesis goal is to understand the phishing process and not quantify and measure the effects of independent variables on the behavior or outcome being studied, the variance approach is thus a limited approach to the phenomena. Although we are to follow the process approach for our RQ, the data provided by these articles still hold great value for our thesis.

The literature review highlights that many theories or models follow a process-based approach. It should be noted that the empirical research or analysis does not necessarily align with a stage modeling perspective. (Abbasi et al., 2021; Abroshan et al., 2021; Canfield et al., 2016; Shaikh et al., 2016; Khonji et al., 2013; Vishwanath et al., 2018; Harrison et al., 2016; Luo et al., 2013). As mentioned previously in this section, a process approach would seek to identify the underlying cognitive processes, learning strategies, or other causal mechanisms that affect individuals in the phishing process. It could explore questions such as: How do individuals apply knowledge to identify phishing? What are the key cognitive processes involved when examining a phishing message? What are the most effective learning strategies to decrease susceptibility?

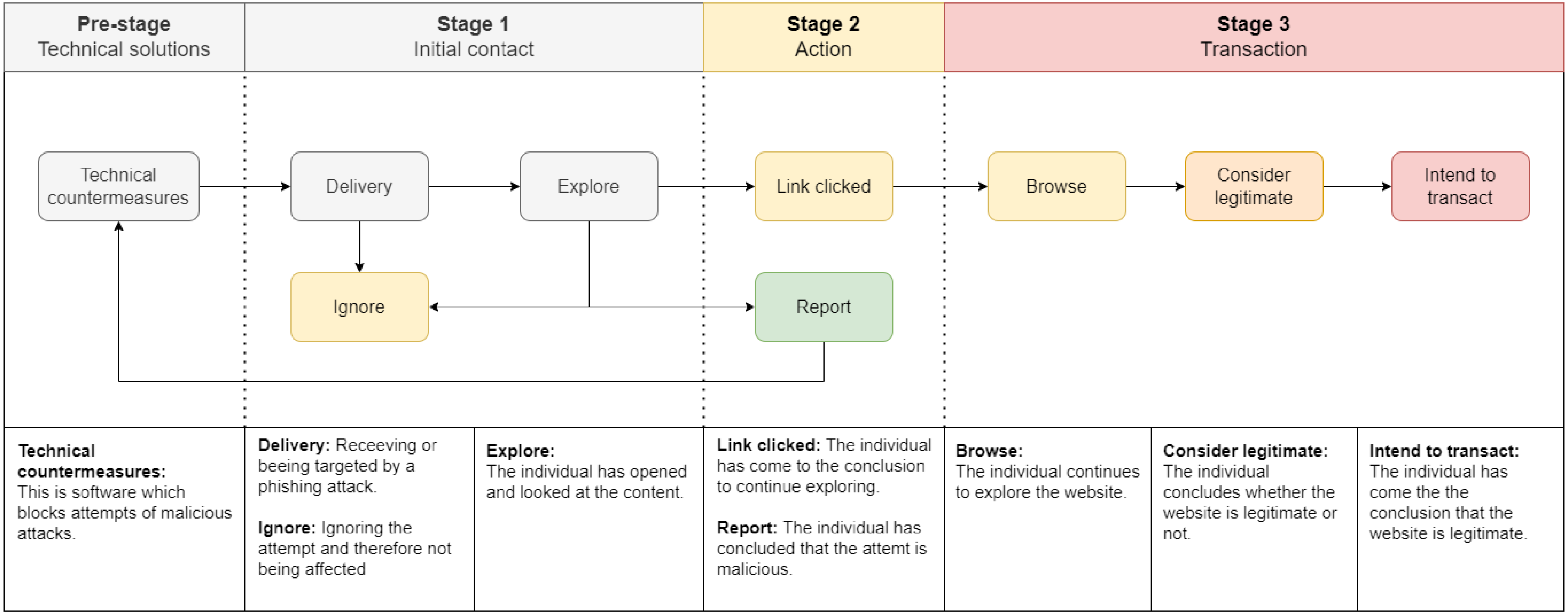
Variance theories and process theories have distinct differences in their areas of focus, breadth, and practical applications. While variance theories aim to account for the variations among individuals or groups in a particular behavior or outcome, process theories concentrate on comprehending the precise causal mechanisms that produce the behavior or outcome. Thus, employing a process approach yields a more intricate and refined comprehension of the causal mechanisms that generate a given behavior or outcome, particularly in complex, dynamic situations involving several causal factors.

Drawing upon this knowledge from prior literature that addressed phishing primarily from a process perspective, i.e., stage model, it becomes apparent that we need to address our approach similarly.

2.7 Preliminary phishing stage model

Our preliminary phishing stage model builds on the literature review above in which the different stages have emerged. The model consists of four stages with constituent activities. The first stage in the model is not the technical solutions explained in the literature review but the initial contact stage. However, we see the need to include technical solutions as a pre-stage to understanding the start of phishing and how an individual can protect against phishing.

As for the model's coloring scheme, we opted for a slightly altered traffic light system. Green represents a beneficial action, yellow means that some control has left the individual, and if the wrong action is taken, it can lead to potentially harmful situations. Orange symbolizes that the potential victim is one step away from a harmful action, while red represents the loss of control and that some harmful actions have already been done.



Technical countermeasures: This is software which blocks attempts of malicious attacks.

Delivery: Receeving or beeing targeted by a phishing attack.

Ignore: Ignoring the attempt and therefore not being affected

Explore: The individual has opened and looked at the content.

Link clicked: The individual has come to the conclusion to continue exploring.

Report: The individual has concluded that the attemt is malicious.

Browse: The individual continues to explore the website.

Consider legitimate: The individual concludes whether the website is legitimate or not.

Intend to transact: The individual has come the the conclusion that the website is legitimate.

Figure 2.3: Preliminary phishing stage model

2.7.1 Pre-stage: Technical solutions

The pre-stage technical solution is based on Khonji et al. (2013) technical solutions for stopping phishing. It is intended in the model to show that not all phishing attempts reach an individual who can interact with it. It encompasses all the technical countermeasures which filter or remove phishing attempts from reaching the targeted receptor. This stage constitutes the technical countermeasures activity.

Technical countermeasures

The technical countermeasure activity is the first activity that can stop a phishing attempt. It can be strengthened by user input through reporting but has no other human interaction. The phishing attempt, if caught, will be stopped and blocked from the targeted receptor.

2.7.2 Stage 1: Initial Contact

The initial contact stage is based on the theory of deception's first stage (Vishwanath et al., 2011) in which the individuals have received some form of deceptive communication through email, SMS, or any other communication channel where the deceptive communication has not been stopped by the technical countermeasures in the previous stage. This stage constitutes three activities. Namely, delivery, ignore, and explore.

Delivery

The delivery activity is where the individual has gotten a phishing attempt from a communication channel, usually email. The attempt can be targeted against them, but it can also be a phishing campaign that technical countermeasures have not stopped.

Ignore

In the ignore activity, the individual can then choose to ignore the attempt and therefore not be affected by the phishing attempt, but this can also lead to the individual ignoring legit communication.

Explore

The explore activity is where the individual has opened and looked at the content of the phishing message, started gathering inconsistencies, and found anomalies that can be used to create a hypothesis. These inconsistencies and anomalies can be leakage cues or other forms of information, such as meta-data, which can give away signs of deceptive communication.

2.7.3 Stage 2: Action

The action stage is the second stage in which the individual evaluates the information so far and comes to a conclusion if they believe the communication. This stage constitutes two activities. The individual has the option to continue exploring by clicking the link or responding to the deceptive communication. They can have found enough leakage cues or inconsistency, which makes them either report the phishing attempt or disregard the phishing attempt and completely ignore it.

Link clicked

The link clicked activity is the action where the individual has concluded that they either would like to continue exploring the deceptive communication or fully believe that it is legitimate and intend to transact with the phishing attempt. This constituent activity is the first place in which what the individual interacts with can cause harm. For example, the individual could want to explore an attachment in the phishing message, which could cause malware to be installed, or click a link that redirects them to a site that hijacks their cookie session.

Report

In the report activity, the individual has concluded that the communication received is deceptive, and they have chosen to report it. When choosing to report the phishing attempt, the technical solution can become aware of the attempt and block further attempts from the attacker. In addition, it will signal to the organization's security department that a phishing campaign might be active towards the organization.

2.7.4 Stage 3: Transaction

The transaction stage is when the individual has chosen to continue exploring the phishing attempt. This stage is directly inspired and influenced by what the literature tells us. More specifically, this stage constitutes three activities. Namely, browse, consider legitimate, and intend to transact. These activities are the three later stages in the phishing funnel model by Abbasi et al. (2021). Although our interest lies in researching the stages and constituent activities that lead into stage 3, it is essential to include these later activities in the model to get a holistic view of the stages an individual goes through. In these later activities, the individual can no longer control what happens. They have left the organization-controlled environment and entered the attacker's domain. The individual will continue to gather inconsistency and create their final hypothesis and conclusion if the website is legitimate and will, in the end, decide if they will give away their information or not.

Browse

The browsing activity is similar to the exploring activity in stage 1, in which the individual will look for more leakage cues that this is deceptive communication and move towards a final decision. However, by exploring the website, they can now interact with potential harmful events, such as malware or cookie session hijacks.

Consider legitimate

When they have reached this activity, the individual will have all the information they need to know if they will interact and give away more information or return to the reported activity in stage 2. If the individual decides to return, they still set their organization in harm's way but have not given away their most valuable information. However, suppose they have concluded that this site is legitimate. In that case, there is a higher chance that the individual will have a transaction with the site and give away valuable information.

Intend to transact

If the individual reaches this activity, they have concluded that the website or attachment is legitimate and intend to transact with the website. The individual will give away the information that the site asks for. However, after transacting with the website/attachment, they can still discover this is deceptive communication and report it, but the harm has already been done.

Chapter 3

Research approach

As our study's objective is to create a model to understand the process or stages better individuals go through when being targeted by a phishing attack, the study needs to address the following research question (RQ):

- RQ: How can we identify and understand the stages involved in the phishing process?

The following section will discuss our choice of approach for this study and the philosophical assumptions that informed the decision by describing the research design "and specific research methods of data collection, analysis, and interpretation" (Chih-Pei and Chang, 2017)

3.1 Qualitative approach

A qualitative approach to research seeks to understand and interpret the experiences, perspectives, and phenomena of individuals and groups. Its focus on subjective experience, the importance of context, and the use of open-ended and non-numerical data such as interviews characterize it. "*All research (whether quantitative or qualitative) is based on some underlying assumptions about what constitutes 'valid' research and which research methods are appropriate. In order to conduct and/or evaluate qualitative research, it is therefore important to know what these (sometimes hidden) assumptions are*" (Myers and Avison, 2002). Myers and Avison (2002) adopted three research epistemologies for qualitative research, which are positivist, interpretive, and critical.

Qualitative research aims to gain a rich and in-depth understanding of the studied subject. It is often done through interpretive methods. "*Interpretive studies generally attempt to understand phenomena through the meanings that people assign to them...*"(Myers and Avison, 2002).

If we align our study's objective with the goal of qualitative research, our objective falls under this explanation. Thus, we are to follow a qualitative approach to address our RQ. Since our study delves into understanding the phishing process from an individual's perspective and, thus, the meaning or steps they assign to the process, our underlying philosophical assumptions would fall under interpretive research. Kaplan and Maxwell (2005) explains it in a way that aligns well with our objective, "Interpretive research does not predefine dependent and independent variables, but focuses on the full complexity of human sense-making as the situation emerges."

Following a qualitative approach gives us flexibility since data collection and analysis are not rigidly decided in advance. That said, the suitable data collection method for our study is to conduct semi-structured interviews. These interviews would give us meaningful insight with detailed descriptions of individuals' experiences, feelings, and perceptions of the phishing process. Furthermore, by conducting the interviews in a semi-structured fashion, the possibility of discovering subconsciously generated stages the individuals went through is open to us.

3.2 Research design

The research questions, the research problem, the theoretical framework, the methodological approach, and the availability of resources should guide the choice of research design. The selected design should allow for the collection and analysis of data that can answer the research questions effectively and efficiently (Creswell, 2008). This study aims to understand the phishing process from the attack target or a potential victim's perspective and, thus, the steps they subconsciously assign to the process. As mentioned in section 3.1 Myers and Avison (2002) pointed out, interpretive studies attempt to understand phenomena through the meaning people assign to them. This resonates with our approach and indicates the stance of our research design.

Following Sarker et al. (2018) map of genres in qualitative research seen in figure 3.1, our study falls under the interpretive case study genre. However, there are variations within specific genres; thus, a certain point on the map can be characterized instead of the genre as a whole. Therefore, we must identify which sub-genre or location on the map our study belongs to. Following the genre and evaluation criteria created by Sarker et al. (2018), our study is located in the red striped area in figure 3.1 since it is both interpretation centric and inductive. The criteria follow four elements that underlay qualitative research genres: data, theory, analysis, and claims. The criteria for this position or sub-genre is to have data as text, theory as a lens or scaffolding, analysis as the empirical elaboration of theoretical ideas, and claims as a new framework or theory that provide novel insight (Sarker et al., 2018).

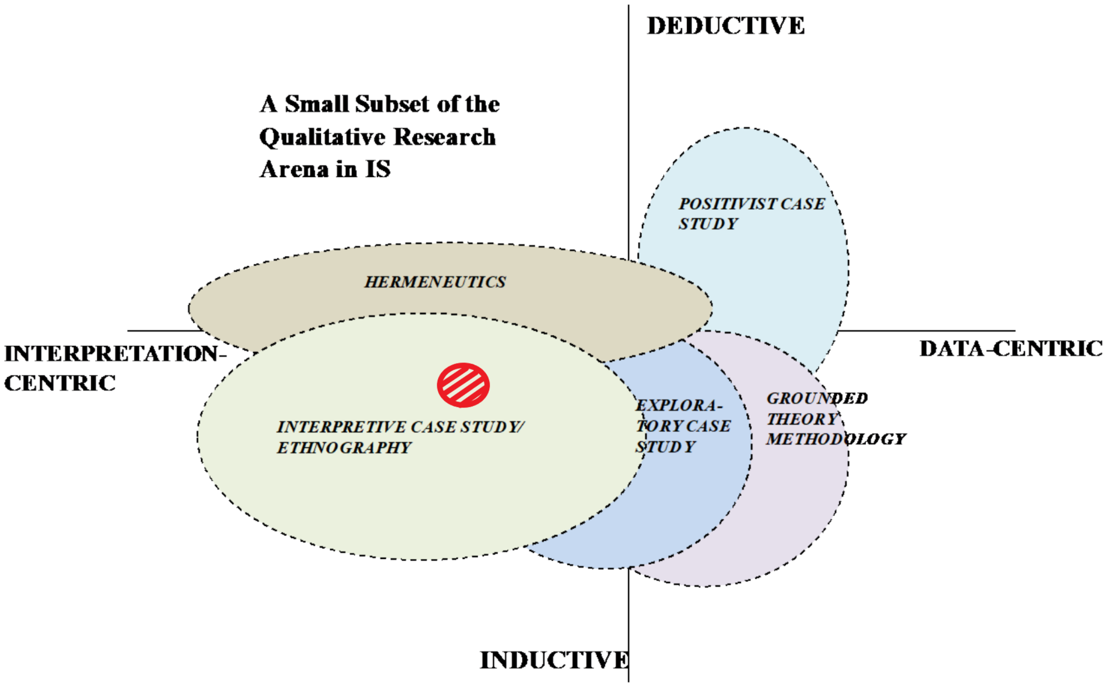

DEDUCTIVE
A Small Subset of the Qualitative Research Arena in IS
POSITIVIST CASE STUDY
HERMENEUTICS
INTERPRETATION-CENTRIC
DATA-CENTRIC
INTERPRETIVE CASE STUDY/ ETHNOGRAPHY
EXPLORA-TORY CASE STUDY
GROUNDED THEORY METHODOLOGY
INDUCTIVE

Figure 3.1: Map of First-Generation Genres in Qualitative Research Sarker et al. (2018) (edited)

To summarize, our research involves collecting data in the form of transcribed interviews, guided by a theoretical framework that informs the study's direction. The analysis process will use an inductive approach, requiring a mental leap from the raw data to form concepts or gain insights. Ultimately, the results of our study will take the form of a model or framework outlining the stages that individuals or potential victims go through during the phishing process (Sarker et al., 2018). Thus this is an inductive interpretive study that takes a holistic approach to the phishing process.

To achieve this, it is crucial to conduct comprehensive interviews and formulate the questions strategically to extract the maximum amount of data applicable to our RQ. Then, by working from these transcripts informed by our RQ, we can synthesize the information effectively and develop a holistic phishing stage model.

3.3 Data collection

Qualitative research aims to examine complex social phenomena by gathering and examining non-numeric data, such as words, images, and observations. The most common method of data collection in qualitative research is done through interviews (Alsaawi, 2014). Interviews allow us to obtain in-depth information from the interviewee about their experiences, beliefs, and perspective on the phishing process and its stages. An interview is a type of conversation that differs from ordinary conversations because it operates under specific assumptions. An interview aims to gather information from the interviewee about their behavior, opinions, experiences, and phenomena. Unlike casual conversations, interviews are carefully planned by the researcher, who typically has a predetermined agenda and specific topics they wish to explore. As such, the discussion is not left to chance, and the researcher will guide the conversation toward their topics of interest rather than allowing the discussion to progress randomly. This method guarantees that the interview stays on track and is pertinent to the research objectives. (Oates et al., 2022).

This study can implement several different types of interviews: structured, unstructured, semi-structured, and focus group interviews (Alsaawi, 2014). Semi-structured interviews "is appropriate for researchers who have an overview of their topic so that they can ask questions. However, they do not prefer to use a structured format which may hinder the depth and richness of the responses"(Alsaawi, 2014, p. 151). Thus we choose to conduct semi-structured interviews.

Doing these interviews in a semi-structured matter allows for flexibility and exploration of the interviewee's answers. Following this method, we can ask follow-up questions to probe for information as necessary to provide a deeper understanding of the interviewee's experiences, beliefs, and perspectives, as mentioned previously Alshenqeeti (2014). This method also provides a certain level of standardization in the questions asked by ensuring that all participants answer the same set of core questions. However, since this approach is flexible, it allows for exploring unexpected avenues of discussion that may emerge during the interview. Overall, semi-structured interviews provided a balance between standardization and flexibility and thus allowed us as researchers to gain rich, detailed data while still adapting to the interviewee's responses.

To ensure the credibility and accuracy of the questions that we planned to ask, we started by reviewing existing literature. This process allowed us to comprehensively understand previous research findings and incorporate them into our questions. Building on existing knowledge from the literature review, we ensured that our interview questions were designed to elicit valuable and relevant responses. This approach also increased our study's overall reliability and validity, as we could draw upon established research and avoid potential biases or errors in our questioning. We created an interview guide based on what we found in the existing literature and created the question with it in mind. The preliminary model also informed us when creating these questions. We had to ensure that the interview questions were relevant to our RQ. Thus the questions were created with what the literature told us in mind.

We have included a table, seen in table 3.1, which presents some information about each interviewee. The sample of our data collection consists of interviews with nine individuals from seven different it consultant firms in the private sector in Norway.

Interviewee	Position	Age	Gender
1	IT consultant	24	Male
2	Identity and access management consultant	23	Male
3	IT consultant	29	Male
4	Security analyst	30	Male
5	Software engineer	29	Male
6	IT consultant	24	Male
7	Department manager	42	Female
8	Senior data scientist and consultant	39	Male
9	Head of department for development and architecture	42	Male

Table 3.1: Interviewee info

3.3.1 The interview process

We contacted multiple IT companies to do the interview process and asked if they had been exposed to phishing through internal tests or legitimate attempts. Of the companies contacted, seven responded positively that they met our criteria. From these seven companies, we got nine individuals available to be interviewed about their experiences.

The interviews were done digitally utilizing the Teams application. This was so that the interviews would be more convenient to schedule in the busy schedules that the interviewees had. This also gave the benefits the application had for recording the interview and automatically transcribing it. When a typical interview starts, we would introduce ourselves and explain what they have given consent to through the consent form. The interviewer would then start the interview, and the other would operate the recording functionality and verify the transcription. These roles would be switched between the interviewer and the transcriber for every interview. The questioning would start when the transcriber gave clearance that the recording and transcription software had started, and the interviewer would start following the interview guide, starting with general information about the interviewee and moving over to the phishing process and its effect. A follow-up question was asked if an answer made light of something new or was unclear. The interviews would end with the interviewer asking the transcriber if they had any questions they might have missed and a general feedback question to the interviewee. The interview would take between 20-30 minutes to complete.

When an interview was done, the interview recording was stopped, and a manual check of the transcription started. The software which automated the process of transcribing had been developed for English and Norwegian bokmål. However, it struggled if the interviewee had a dialect or talked quickly. Therefore a manual check was required to fix some of the lines, which was done by re-watching the recording and fixing the mistakes in the transcription.

3.3.2 Interview limitations

There are several limitations when conducting semi-structured interviews in qualitative research. One limitation is that the researcher's biases may influence the results, as the researcher can guide the interviewee's responses in a particular direction. Another area for improvement is that the data collected may be limited to the interviewee's perspective, which may not represent the views of the broader population. Additionally, there may be issues with reliability and validity, as the same questions may be interpreted differently by different interviewees. Finally, the time and resources required to conduct and transcribe interviews can be significant, making collecting data from a large sample size challenging. Nonetheless, the limitations were considered during the interview process, and the aforementioned interview guide was created.

3.4 Data analysis

Inductive analysis is a method of data analysis in qualitative research where the researcher develops theories and models from the collected data instead of testing a preexisting theory (Thomas, 2006). In this case, the aim is to synthesize the interview transcripts to identify subconsciously generated stages in the phishing process. First, the interview recordings were transcribed using Microsoft Teams transcription software. Once transcribed, the data is coded using Nvivo, a software program that helps to organize, manage, and analyze qualitative data. The codes are created from what we learned from the existing literature during the literature review and derived from what the interviewee says during the interview. This process of inductive analysis helps to ensure that the research is grounded in the participants' experiences and perspectives, providing a more comprehensive understanding of the research topic. The findings section provides a summary of the responses, which are subsequently juxtaposed with the existing theories and findings from the literature review in the discussion chapter.

In this study, we adopted the strategy of inductive analysis suggested by Thomas (2006). In this strategy, there were five steps we had to follow. It started by preparing the raw data files, or in other words cleaning the data. During this step, we also cleaned the names and other identifiers from the files. The second step was to read through the raw text in detail until we were familiar with its content and gained insight into the themes and events covered in the text. The third step we followed was creating categories and themes we had identified from the interviews. As previously mentioned, we did not only rely on categories derived from the interview texts but also from what we learned from the existing literature. The fourth step consisted of us reducing overlapping codes, since following this process, a text segment may be coded into several codes, as well as reducing the redundancy among the different categories of codes. The fifth and final step in our process consisted of us continuing to revise and refine the category system. As Thomas (2006) mentioned in his article:

> *"The intended outcome of the process is to create a small number of summary categories (e.g., between three and eight categories) that in the evaluator's view capture the key aspects of the themes identified in the raw data and are assessed to be the most important themes given the evaluation objectives."* (Thomas, 2006, p. 242)

We followed the aforementioned five steps to develop eight important themes or categories from our nine interview transcripts. These eight core categories have a few underlying codes for each stage in the phishing stage model. What determined the inclusion in these codes for the stages depends on the context given by the interviewee. Several text segments presented themselves as part of a stage in the phishing stage model, for instance, "A few emails have been received which should have been filtered out, which then came directly. I reported those to the security department.". This text segment fits into two different codes. The first part falls under the preface technical solution, while the later part of the segment emphasizes the report stage in the model.

3.4.1 Analysis limitations

Inductive analysis in qualitative research has several limitations. First, it can be subjective, as it relies heavily on the researcher's interpretations of the data. This subjectivity can lead to different researchers coming up with different conclusions from the same data. Second, inductive analysis can be time-consuming and resource-intensive, requiring careful review and analysis of large amounts of qualitative data. Third, it may be difficult to generalize the results of the inductive analysis to larger populations, as the sample size in qualitative research is often smaller and more focused. Finally, there may be limitations in the quality of the data collected, such as bias in the selection of participants or the quality of the interviews themselves, which can impact the validity of the findings.

3.5 Ethical considerations

To conduct scientific research, we have to gather data. In our case, this is done through interviews. Confidentiality has to be considered when interviewing people since we collect personal information. Although our research does not involve extensive sensitive data, specific details such as names, organizational roles, and contact information must be protected. To ensure the security of this information, all interview materials, including recordings and transcripts, are stored on encrypted and safe cloud storage provided by the University of Agder. The interviewee has the right to revoke their consent at any given time, in addition to the right to gain insight on any stored materials they have provided.

We needed to apply to the Norwegian Agency for Shared Services in Education and Research (SIKT) to store and collect information from our interviews. SIKT is responsible for handling all research projects and maintaining an archive of research data. Their website states that they *"provide a shared infrastructure for Education and Research that ensures excellent user experiences in compliance with our general goals for digitization, data sharing, and open research."* (Sikt, 2023). We ensured that our application to SIKT was approved before starting the interview process and collecting and storing any data.

Chapter 4

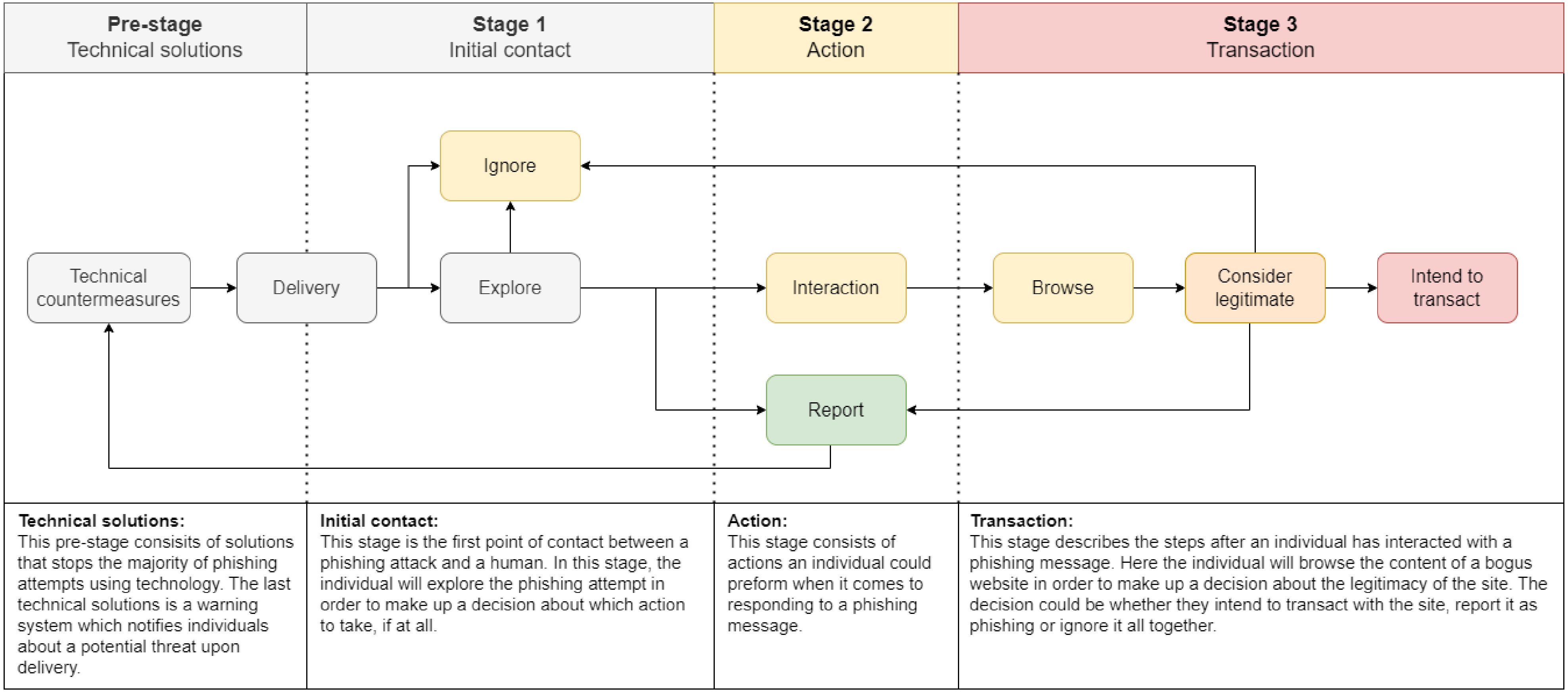
Findings

Concerning our RQ, "How can we identify and understand the stages involved in the phishing process?" We have made significant discoveries regarding phishing attacks, yielding several key findings.First and foremost, we have identified that warnings during the delivery stage play a critical role in preventing users from falling prey to phishing scams. Secondly, we have discovered that users tend to report phishing both officially and unofficially. Additionally, we have found that some ignore phishing emails altogether. Another important aspect we explored is the information processing strategies employed when evaluating the legitimacy of a message. Lastly, we identified manually entering a URL as a valuable technique for avoiding phishing attacks. From these findings, we developed a revised phishing stage model. In the following sections, we will provide a more detailed analysis of each of these critical findings, beginning with findings in stage 1 of the model and its constituent activities, before venturing down the stages in stages 2 and 3 in the following sections and later discuss these in the subsequent chapter. By structuring our empirical findings in this manner, we can offer a comprehensive context for comparison and discussion in the following chapter, aligning it with the proposed phishing stage model and the theoretical framework utilized.

4.1 Revised phishing stage model

Initially, we had a theory-driven understanding of what a phishing stage model would look like. The preliminary model was created from our understanding of the literature, and thus when we analyzed the interviews, some changes had to be made to the model. Figure 4.1 shows the revised phishing stage model. The main change from the preliminary model to the revised one is the change of focus from the constituent activities to the main stages. Thus the descriptive part of the model changed focus from describing each activity to describing the four main stages, i.e., the pre-stage, stage 1, stage 2, and stage 3. In addition, in stage 3, two arrows point from the consider legitimate activity to the report and ignore activity to emphasize the different paths that can be taken. In addition to this the link clicked activity changed name to interaction in order to encompass different kinds of interaction, such as clicking a link or opening an attachment.

The following sections are structured after the revised phishing stage model shown in figure 4.1. First, we will describe the pre-stage and then delve into the different findings that support the constituent activities that comprise each stage.



Technical solutions:
This pre-stage consisits of solutions that stops the majority of phishing attempts using technology. The last technical solutions is a warning system which notifies individuals about a potential threat upon delivery.

Initial contact:
This stage is the first point of contact between a phishing attack and a human. In this stage, the individual will explore the phishing attempt in order to make up a decision about which action to take, if at all.

Action:
This stage consists of actions an individual could preform when it comes to responding to a phishing message.

Transaction:
This stage describes the steps after an individual has interacted with a phishing message. Here the individual will browse the content of a bogus website in order to make up a decision about the legitimacy of the site. The decision could be whether they intend to transact with the site, report it as phishing or ignore it all together.

Figure 4.1: Revised phishing stage model

4.2 Pre-stage Technical solutions

The pre-stage marks the initial stage of the phishing stage model, serving as its starting point. In this stage, the focus is on employing technological solutions that thwart most phishing attempts. A crucial component within the technical countermeasures activity is implementing a warning system, which promptly alerts individuals to potential threats during delivery. Hence, the delivery activity is interconnected with this pre-stage.

4.2.1 Technical countermeasures

Some of the interviewees mentioned technical solutions and how the solutions worked when they were describing phishing. They would describe it as a filter that let potential phishing emails through, and they all had different opinions on how this filter worked. This finding also gave us insight into another way the technical countermeasures affected them. The countermeasures would affect the interviewees into the delivery stage by warning them that the email received was from an external source outside of the organization. The service would then add a warning label to the email, making the interviewees more aware of the email.

> *"I do get a warning that "This is a person you don't often get an email from so be careful". When I first get a warning I become a bit more careful, right? So when I am already warned then I will thread more carefully."*

Interviewee 1 explained that the warning they got when an email was sent from some external source they did not often communicate with, and that this warning made them more aware of the email.

> *"Yes we get a warning when we receive an email from outside of the organization but also when we send an email to an external recipient."*

Interviewee 7 talked about the technical countermeasures, and when asked if they got a warning, they confirmed that they got a warning on any received email from an external source. However, they added that they also got a warning when they emailed someone outside the organization.

When discussing their experience with phishing, Interviewee 7 opened up with how they thought the technical countermeasures worked and how it has protected them from phishing attempts.

> *"A few emails have been received that should have been filtered out, which then came directly. I reported those to the security department."*

In addition to this, Interviewee 8 also mentioned technical countermeasures during the interview.

> *"and it surprises me because it has been pretty little phishing for a while. But that can also be that I have started to use my private email more for online services and that I have gotten used to the filter taking all the attempts. So I have really thought that what's going through should go through and that what's not supposed to go through gets blocked. However, I have felt split about that conclusion as I have noticed that good email gets stopped and bad email goes through."*

Here the interviewees talk about how the filter has prevented what they expect to be multiple phishing attempts. Interviewee 7 talks about how only a few have gone through the filter and that the few that did they could easily spot on. Interviewee 8 discussed more on how the filter has become so good that they, for a while, did not feel like they had gotten any phishing attempts, but when they then started to use their private email more actively, they found that the filter was not working as strong as they had believed. This resulted in them theorizing that the filter worked, but not at all times, so that some emails would be flagged when they were good and some bad would be let through.

4.3 Stage 1 Initial Contact

This is the first stage where the human element first comes in contact with the phishing attack. The stage revolves around exploring the content of the phishing attempt in order to make up a decision about which action to take, if at all. The stage constitutes three main activities. Namely, delivery, explore and ignore.

4.3.1 Delivery

All of our interviewees explicitly mentioned the delivery of a phishing attempt over email. In addition, Interviewees 1, 2, 3, and 9 mentioned another delivery method, namely SMiShing. Firstly Interviewee 1 made a distinction between receiving a phishing email privately and in a work context before they talked about their knowledge of phishing and its delivery methods:

> *"There is a lot of phishing that happens privately, outside work. It is both in the form of messages on the phone and links in emails that are sent. But in relation to work, it was only one case that I remember. There was an administrative email that was sent out, where it says I have to click this link to update my profile on this thing."*

Interviewee 2 further backed up what Interviewee 1 said by stating:

> *"It's a form of social engineering to trick people into giving away knowledge. It's probably most common in email and SMS, I think. So yes, it's just a form of getting sensitive information."*

During the interview with Interviewee 3, they further supported the inclusion of delivery as a stage by saying that a phishing attempt consists of someone receiving an email or getting a text message where the goal is to get the potential victim to click a link. When asked about what they knew about phishing, they stated:

> *"I know that it is widespread. Such email phishing attempts are typical. Receive an email, and then someone tries to get you to click on a link, or you get a text message where they are trying to get you to click on a link that may appear to be from someone you know or from a service you are familiar with. They often appear after you have used similar services."*

Importance of warnings

During the delivery stage, we also found that individuals rely on technological tools to alert them of potentially malicious emails. There are several findings from the interviews that supported this, as Interviewee 1 put it:

> *"Consulting firms are doing quite well with handling phishing. I get a notification that you don't often get an email from this person, so be careful. I got it when you*

> *sent me an invitation to the teams meeting, I got notified that I had something I needed to potentially be careful with. ... Once I get a warning, I pay attention, right? When I have already received a warning that there might be something, I am careful. Take them with plenty of time usually."*

Additionally, Interviewee 2 supported this finding by stating that:

> *"There is always a red warning label on emails that are not sent from the company internally. So the first thing I see is that oh look at the red text. Then I get reminded that ok, now I really need to double-check this email."*

4.3.2 Ignore

We found through the interviews that some interviewees actively chose to ignore the phishing attempt, either by seeing the email and just ignoring looking at it or that they deleted or blocking the email without reporting it into the system. The interviewees who mentioned ignoring were predominately the younger ones, and when asked about what they did when they identified a phishing email, Interviewee 1 stated:

> *"...since I knew it was phishing I didn't do anything more with it, but usually I would of course block and delete it. "*

The statement from Interviewee 1 shows that the knowledge that they should report is not necessarily there.

To build up this finding that ignoring emails is prevalent, Interviewee 2 showed an attitude likewise to Interviewee 1 in that if they are insecure, if the email is phishing, they will ignore the email. When Interviewee 2 was asked why they chose to ignore the email, they answered that they did not see any negative consequence about ignoring it but rather the negative consequences of clicking something unknown:

> *"and it is like, I have this precautionary principle that if I am insecure about it, then I'll ignore it."*

Interviewee 2 states that they would rather ignore an unknown email than risk doing something that could harm them or their company. This means that they will ignore the email. However, they never mentioned reporting it as an option, showing that their company either does not have a procedure for phishing or that they lack knowledge of the procedure. Specifically, Interviewee 2 stated that:

> *"What do I lose by ignoring it? And what do I lose if I fall victim to a phishing attack, especially on my work email? I'm not gonna open something I don't know what it is."*

Interviewee 5 said something which differed from Interviewee 1 and 2 in which they knew the procedure but did not comply with it:

> *"Unfortunately, I have sadly sinned. I have not reported it because you are exposed to quite a large amount of it in private at least. So then I just delete it."*

Interviewee 5 stated that they know what they are supposed to do but lack the motivation to do so and, therefore, actively choose to ignore the phishing attempt. He explained that it comes down to over-exposure of phishing emails on his private email, where the procedure is to ignore usually, and that this procedure has leaked over in his work environment, thus making it probable that the phishing email is ignored instead of complying with proper procedure and reporting it.

Interviewee 6 differs from the rest of the answers in that they willingly inform that they choose to ignore because of their "lazy" personality and the perception that everyone knows that they should not press the button/link, ending with an egocentric thought that is long as they do not press the link. They would not care.

> *"Hmm I am too lazy I recon, It's like everyone knows that you shouldn't press it so as long as I don't press it, I don't care."*

Reasons why they ignore

Going back to the first quote in this section, Interviewee 1 explained that since he recognized it was a phishing attempt, he did not feel the need to do anything about it. However, he would typically block and delete the email. Interestingly Interviewee 1 mentioned that he had received little to no training. Interviewee 2 further backed this by mentioning that he usually ignored emails he recognized as phishing. Neither of these mentioned reporting in any way or form. This shows that the knowledge that they should report phishing attempts are not necessarily there. Instead, they ignore the email by blocking and deleting it. In addition, Interviewee 6 explicitly stated that he is too lazy, showing a lack of training and great trust in technical solutions.

This lack of knowledge is supported by the interviewees mentioning that there is a lack of training on phishing. Five out of nine interviewees explained that they had not received any formal training related to phishing in any form. One Interviewee who mentioned training was when we asked, Interviewee 4 about it he stated:

> *"... it's more of a verbal review of the course of events of phishing emails and not direct courses, but more of experience and knowledge sharing among colleagues"*

Interviewee 2 explicitly mentioned that the amount of training is lackluster and that companies should prioritize training. He explained what training they had received:

> *"Just general training about it in some meetings and things like that where it is a reminder to be careful. But I actually think there has been too little of it. Too little training on what it is. Everyone at my job is pretty good at that sort of thing already, but still, you have to have a reminder once in a while, and there has been too little of that, I think."*

Although there has not been any formal training among the seven different companies, three interviewees mentioned phishing tests done internally when asked about training. In addition, three of the older interviewees said they had undergone training at a previous workplace or through a subject group based on interest.

In addition to the lack of training, Interviewee 6 mentioned he also expressed a high level of trust in institutions, his workplace, and websites and that they would ensure his and his personal information's safety. He explicitly stated:

> *"I trust that the state of Norway has enough money to create good and secure solutions."*

4.3.3 Explore

During the interviews, we found evidence that supported the exploring activity in the phishing stage model. All the interviewees mentioned that the first thing they did after receiving an email was to explore the content and look for leakage cues.

Overall impression

Several interviewees mentioned that the overall impression played a crucial part during this stage, in addition to leakage cues. During the interview, when talking about how he explored emails, Interviewee 2 stated:

> *"It was just the overall impression. I think I just googled the content to see if it is legit, do they ask you about this around this time? I also looked at how the email was written. I wonder if I googled the email address itself as well. And also I have a precautionary principle, so if I'm unsure, I ignore it. ... I always think about whether this could apply to me. And then there is the overall impression. If I am in doubt, I read through everything. I know those guys(attackers) write bad grammar."*

Leakage cues

Even though the overall impression plays a part in identifying phishing, "There are always some hints" as stated by Interviewee 6. Another interviewee further elaborated on this during the interview with Interviewee 4. He stated that he would:

> *"Double check the sender by looking at the domain used instead of just looking at the heading of the email, in fact-checking the sender."*

Common among the interviewees was that they had the knowledge that they should look at the sender and hover over links to see the full URL and the wording of the content. Even though all interviewees had this knowledge, Interviewee 6 still fell victim to a mock phishing attack. As mentioned previously, Interviewee 6 spoke of there always being hints that give away a phishing email. They further elaborated on why they fell victim to the attack

> *"It was a test at the customer, and it was the first phishing test there. I was a bit stressed when receiving emails from them, I guess, and it was a lot more personal too. I should have realized what it was. So then I clicked the link. I just wasn't as alert at the time."*

Knowledge of company policies

Additionally, looking for leakage cues, we found that those aware of company policies have a greater chance of not falling victim to phishing. Interviewee 4 said this when talking about a phishing test they had done:

> *"There was a phishing test in the period when LastPass(a password manager) had been hacked and I think customer data was leaked. So the test was based on this. They pretended to be LastPass and said that there was gonna be some kind of update across the organization, but I knew that the policy in our organization does not include a standardized password manager. So when I got told it was coming and that I had to press this link to update, I knew it was shady. We have a separate internal security team who said this was phishing very quickly and that confirmed my suspicion."*

Information processing

When we asked the interviewees about their thought process when exploring an email, Interviewee 8 provided insight into both when they realized an email was phishing and once when they failed to recognize an email during a phishing test:

> *"Yes, so the time I failed the phishing test. It was simply that I had looked at an email just before that which was not phishing. Where in a way some alarms had rung and then I pressed anyway, so it was simply the one time my intuition didn't tell me I had to check. ... as soon as there is suspicion, then there are the natural checks to see if the sender is, in a way, a reasonable email. Often there are very long, complex emails. Otherwise, you have to look at the email itself and see if there are grammatical errors or pictures or links."*

Here Interviewee 8 states that intuition plays a crucial part when exploring an email and that they further explore the email to identify leakage cues as soon as there is suspicion.

When asked about their time use during this process, Interviewee 8 made a distinction between when they worked at a company that regularly sent out phishing tests and where they are working now:

> *"Now it has become so good that I can. I think it takes less than 3 seconds. Whereas when I worked for a company that sent tests constantly, the emails were in a way on the borderline. Then I might take up to 20 seconds at the worst."*

4.4 Stage 2 Action

The action stage revolves around an individual's actions when responding to a phishing message. Should an individual venture this far, their action would be informed by their exploration during the previous stage. The stage constitutes two main activities. Namely, interaction and report.

4.4.1 Reporting in more ways

In the interviews, we found that the interviewees reported phishing in quite different ways. For example, they would ask the person next to them if the communication received was legit and discuss it with them, or send the email into a collective group communication application. In addition, some would report the email through the technological system, which we refer to as the official system, that follows the organization's policy on phishing reporting. Finally, a few would know that they should report the email but still choose to ignore the email.

Reporting through the official system

When asked about how they discover phishing, Interviewee 3 responded with a longer explanation in which they use leakage cues such as the domain URL for the email address to verify the email authenticity and if they cannot get a read on the authenticity of the email from the URL they would check the meta-data. As a follow-up question, we asked them how they would react if the email were phishing, and they answered:

> *"If i get it on my job email, then I'll mark it, and they should go automatically into something central, and then the email... gets shared with the rest of the system and then it's blocked for everyone... I think. "*

Interviewee 3 responded that they would react by reporting the email using the built-in report system, and they thought that the phishing email would go into a central database which would share the email with the rest of the system and therefore block the attempt for everyone else. When asked why they chose to report the email, they responded with this:

> *"No, that is. It is because it is simple, as it is easy to report, and it is part of our routines internally."*

They chose to report the email because it was, in their mind, easy to report and a part of their internal routines. A finding that can explain why people may choose to report through the system for which it is built. Interviewee 4, when asked the same questions, answered that he would report, but because of external factors, he could not. This could show that reporting can be linked to having the available tools at ease.

> *"Personally, I didn't get anything done as I was actually sitting in the middle of a meeting. But if I had been at home, as I have done before, I would actually click on the report, i.e. report as phishing. But in this particular case, I couldn't do anything."*

Reporting through an unofficial channel

Throughout the interviews, multiple forms of unofficial channels for reporting have been discovered. These unofficial channels are all from chat groups to the people around them and go around the official system the organization has set for phishing to be reported. One of the interviewees even mentioned that they talked with the security department but did not report the phishing attempt through their communication system.

When we asked how they reacted after discovering the phishing attempt, interviewee 1 said they would take a screenshot of the attempt and send it to a collective chat group in the company.

> *"Laughed, Yes it was very obvious... I just took a screenshot, and then I sent it to a collective chat group at work and said now we have started."*

The context of the quote is that Interviewee 1 was informed that the organization might have a phishing test, and the Interviewee figured that since it was October, also known as the security month, the test would be done then. As they explained in the quote when they discovered it was phishing, their first response where to laugh and then take a screenshot and send it to their work chat group, informing the group that the test had begun. However, there are other ways the interviewees inform their other employees. For example, some said they would ask their neighbor if it was a phishing attempt. First Interviewee 5 states that:

> *"In a work context, if more of my colleagues say they have gotten dodgy stuff, then I will use that as an identifier."*

Interviewee 6 added to this by stating:

> *"I just talk to the people I work with, and then I am like. Hey! Have you also gotten this email or something like that, ask them if it is like phishing. They will answer yes that is phishing."*

Both answers above show that they discuss with their colleagues or get warned by them if there is an attempt at deceptive communication. Interviewee 6 explained in greater detail that he would actively talk to colleagues when they felt something was off with the email. In contrast, Interviewee 5 was more informed of potential threats by colleagues. Both of them use their surrounding colleagues to become more aware of threats or identify threats.

4.4.2 Interaction

We found empirical evidence supporting the interaction activity's inclusion during our interviews. Since all interviewees mentioned, either directly or indirectly, that the goal of a phishing email was to get an individual to interact with a phishing message by clicking on a link. When asked about what they know about phishing, Interviewee 3 said:

> *"I know it's widespread. Such mail fishing attempts are typical. You get an email, and then someone tries to get you to click on a link, or you get a text message. Trying to get you to click on a link that may look like it's from someone you know or from a service you're familiar with. And they often appear after you have used similar services then."*

Another Interviewee who answered similarly to the question was Interviewee 5, who stated:

> *"I know of phishing emails and the usual thing is that you click on a link, and then you end up somewhere and then you fill in things on websites you think are legit and log in. ... It looks sketchy, and maybe it's a service that you don't use. You often see it on links and how it is worded. And usually, it is always better to enter via URL instead of the link. You know, instead of clicking on links in emails. It's rarely a good thing to do."*

Both interviewees quoted above clearly emphasize the action of clicking a link supporting it as a stage in the phishing stage model. In addition, during the interview with Interviewee 8, he mentioned that if he had not recognized an email as phishing and clicked a malicious link, he would have noticed it once he had seen a redirect. He further explained that some damage had already been done by clicking:

> *"The first thing that happens is that it pops up, I would have seen a redirect and then it would have been over. But what happens then is that they would have gotten the scent of blood. Then they would have known that the email belonged to someone who could be receptive. So then I would have reported it and in a way be a little more careful in the future. ...I don't think it would have gone any further than that if I had seen the URL kind of kick. But what I had noticed would probably be that I had to be very careful, maybe for the next year or 6 months."*

Manually enter URL

In addition to mentioning the link clicked stage, Interviewee 5 explained that it is better to enter a website by entering the URL instead of clicking on a link in the email. Interviewee 2 supported this finding by stating:

> *"... I never click on a link or anything. If they're requesting sensitive information, That is often what they are looking for. It's like that if they ask for passwords or bank details immediate red flag."*

Another Interviewee who mentioned this was Interviewee 7. During the interview, they used ordering packages online as an example. They often did so, and when ordering online, you often get an email where you can track your order. They had received several emails where a threat actor impersonated DHL and sent out phishing emails with links to "track" the package.

> *"If there is tracking, I would rather go to the page of the supplier and track my package from there. So I might be a bit more skeptical than average."*

They further elaborated that they only did this if they actually had ordered a package and were waiting for it. Had they gotten such an email from "DHL" when they had not ordered anything, they would never have bothered to open it. This shows that a highly specific phishing email will, in some cases, be seen right through. While in those few cases where the specific content hits, it can be fairly difficult to identify the phishing attempt

Knowledge of common practices

Another interviewee elaborated on this by mentioning that having knowledge of common practices from institutions dealing with sensitive information can spoil the phishing attempt. Interviewee 4 stated that he would:

> *"Look at the sender. Double-check the sender by actually seeing the domain used to send the email. Not just the header from the email, but actually check the sender. Based on what the email is about, it is possible to check, for example, The Norwegian Tax Administration, they will never have a link in their emails. So if we then receive an official email from the tax administration or post office, there will never be a link in these emails."*

Possessing the knowledge that these public institutions never send emails with links can prevent potential victims from venturing to further stages. Had he not possessed this knowledge, he would have had a greater chance of traversing to the next stage in the phishing stage model, namely browse.

4.5 Stage 3 Transaction

The final stage revolves around the steps taken after an individual has interacted with a phishing message. The stage constitutes three main consecutive activities. Namely, browse, consider legitimate, and intend to transact.

4.5.1 Browse

During our interviews, one of the interviewees explained the phishing process in one sentence:

> *"I know phishing emails and the usual thing is that you click on a link, and then you end up somewhere and then you fill in things on a website you think are legit and log in and it stops there."*

Interviewee 5, in the quote above, mentioned several of the activities in the previous stages, such as delivery, although he did this indirectly, and link clicked, as well as the browsing activity in stage 3 and its subsequent activities, which we will present our findings on in the following sections.

What we found during our interview with Interviewee 7 was that when they were unsure of whether or not a link was malicious or not, they would use a separate family PC that was not connected to her workplace or contained much sensitive data and browse the content of the website there:

> *"I don't click on links unless I know it's going to be an email from a confidant. I have a PC that the children use, and then I can just forward the email and open it there. But it's very rare that I take that chance. It is often the case that I am very sure, and know that it is nothing, but if there is a small percentage of risk, then I take it instead on the other PC, but otherwise, if it is a trusted person, I know that the mail is coming from, I'll click on the link myself instead."*

During our interview with Interviewee 7, they walked us through the stages they think one is going through when being phished. For them, the process stops at explore since they would have expanded the details from the sender and checked the links before she reported the email. But they further explained that they could have clicked the link and entered the website if they had been more gullible. Once there, they would have browsed around and looked for further leakage cues, such as if they asked for information they really should not have:

> *"... If I had been a bit gullible and clicked in, and they ask me for some information that they really shouldn't have, then it would have stopped at the web page I was on"*

We found further evidence that supported the browsing activity in our interview with Interviewee 9. When asked about what they thought would happen if they had not recognized an email as phishing, they explained that they most likely would have been routed to a website of some sort:

> *"... probably had been routed to some website which might have looked similar to real ones, for example, or typically some website where one is supposed to be verifying some bank account, information or something."*

4.5.2 Consider legitimate

Going back to the quote from Interviewee 5 in the previous section where they mentioned that you enter a website you think is legitimate. The key part in his statement is "a website you think is legit." This implies that there had to be a stage beforehand where you gathered data to make an informed decision in this stage on whether you consider the website legitimate or not. The websites in question are often made to look similar to the original website. As stated by Interviewee 9:

> *"...a website that might look similar to the original site."*

Since these websites try to appear legitimate, according to Interviewee 8, the clue to doing so is to be highly specific from an attacker's perspective. By being specific, those not in question would have a greater chance of identifying it as phishing and not considering it legitimate. In comparison, those who fall under the narrow umbrella of the specific website have a greater chance of considering the website legitimate.

> *"... for most people, it will appear completely silly, but for the person whom they exactly meet the need, I think they knock through a part of those filters you have. ... Is there someone who had sent something to Verizon 2 hours ago, then it fits very well with the mindset you have. I think they are pretty good."*

4.5.3 Intend to transact

For the last activity in stage 3, several interviewees ended their description of the phishing process by saying, in one way or another, that the last step was to transact with the website they had been redirected to. Thus, intent to transact is the last activity of the phishing stage model. As Interviewee 9 put it, the goal is to

> *"...try to retrieve personal information in a way as I reckon that has to be the purpose of most of them in a way. Yes, get a hold of your personal information or a credit card or any other sensitive information."*

During the interview with Interviewee 5, they also mentioned that the last step was to transact with the website:

> *"... you fill in stuff on websites you think are legit and log in. And, it stops there."*

What he meant by stuff in the quote above can be assumed to be personal information or other sensitive information since he also mentioned that you "log in" and thus give away said information. Alternatively, in other words, you intend to transact with the website.

4.6 Changing risk perception between work and home

As mentioned in 4.3.1 Delivery, there is a difference in how the interviewees have looked at phishing attempts on their private email compared to the organization's email. The interviewees answered slightly differently when they handle phishing attempts on their organizational email, and they are more aware of the potential risk than when they get it privately.

> *"Yes because it's more active. There is a greater wish to gain access to our work system and to add to that when I am in private I usually use software produced by bigger professional companies, while when I work I am often in a smaller company which have not necessarily configured their software just as good."*

When asked if the risk changes from private to work, Interviewee 8 answered yes, and gave the reasoning that there is a more significant gain to attacking the organization than them. This makes them more aware of potential threats when they are on their work platform than privately.

> *"It's pretty much the same but there is a higher chance that you would get targeted at work where you sit on sensitive information, so in that way, it's a greater risk to get caught at work."*

Interviewee 5 thought that the risk was in the same class but that there was a higher chance of getting targeted in a company, and that there was a higher risk of getting caught.

> *"No, I think it's ... I think it's pretty high anyway, and at a personal level there are more scams, which I think there are a lot of people who work in a company that goes on."*

Interviewee 6 meant that risk was high regardless, and people who get scammed privately often also work in an organization.

> *" Fifty-fifty for the everyday man. They don't have that safety net in place at their homes which they have at their workplace, so you are better secured at work because for example outlook filters out a huge amount of email for an organization, and your private email does not necessarily do it."*

Interviewee 7 stated that there was not much of a difference in risk but said that the organization's technical solutions and safety net made it more secure for potential threats than privately.

Chapter 5

Discussions

This study aimed to develop a holistic phishing stage model that comprehensively captured the nuanced process or stages that individuals go through in the phishing process. By doing this, we aimed to shed light on the psychological, behavioral, and contextual dynamics that impacted individuals' experience and decision-making during a phishing attack. Following an interpretation-centric and inductive research approach, we constructed a theory-informed model following the theoretical framework to create an iterative understanding, resulting in a revised model informed by our findings.

In this chapter, we dig into the detailed discussion of our findings by presenting an in-depth interpretation and analysis of the stages individuals go through during a phishing attack by highlighting key themes, sub-themes, and patterns that emerged from our data. We aim to provide a nuanced and comprehensive understanding of a phishing attack by integrating these findings into our holistic phishing model. Thus we contribute to the growing body of knowledge aimed at enhancing cybersecurity practices and mitigating the impact of phishing attacks.

5.1 Theoretical implications

Theoretical implications are an integral component of the discussion chapter in this thesis, as this section provides a deeper understanding of the broader significance and contribution of the research findings. In this section, we discuss the implications of theories and concepts touched upon in our literature review. By exploring the theoretical underpinnings in relation to the empirical findings, we aim to shed light on the implications for existing theories and models.

5.1.1 Phishing stage model

The phishing stage model encompasses elements from the different stages models presented in the background and related work 2. The work of Abbasi et al. (2021); Abroshan et al. (2021); Burns et al. (2013) affected the entire process of developing a holistic phishing stage model. The PFM from Abbasi et al. (2021) predominantly informed stage 3 in our model, while Abroshan et al. (2021) three-step process to phishing informed the delivery, explore, interaction, and intend to transact activities. Burns et al. (2013) work on SASM further supported the interaction activity and informed the movement between stages and activities. This model can be considered a reversed form of the cyber kill chain, as it can be called a phishing kill chain. What is meant by this is that while the cyber kill chain is a step-by-step approach looking at how threat actors can be stopped, the phishing kill chain looks at it from the victim's perspective and presents a step-by-step approach to how the victim might fall for a phishing attack.

5.1.2 Hindering phishing (Pre-stage)

The pre-stage(technical solutions) is included to show that there is a technical stage before any human interacts with a phishing attempt, but it is not a complete stage of the model. This stems from the model's focus on the stages an individual would follow when interacting with a phishing attempt. However, the pre-stage gives context to how an individual would end up interacting with phishing if it were to fail, and it is essential to include it in the model.

Technical solutions in more stages

Throughout the findings, a technical solution was discovered, in which the individual would get a warning label on all emails from an external source, which for some individuals, increased their awareness that this might be a phishing attempt. Our literature review did not cover this and affected the model in which the technical solution became a static pre-stage.

The technical solution pre-stage was validated in findings when a filter system much like the blacklist solution mentioned by Khonji et al. (2013) and Butavicius et al. (2022) was discovered. The data from the findings suggested that individuals could feel that reporting the emails had caused fewer phishing attempts over time and that the filter system worked. Some might even think that the technical solution has become so good that they will not receive phishing attempts. However, this might come from using software from more prominent organizations with more resources and knowledge about the proper configuration.

The findings mention a warning label placed at the top of each email received from external sources or from individuals not often communicated with. This warning could make some individuals more aware of potential phishing attempts. It made it more transparent for the receiver that this was an email from someone outside the company or that the sender was someone they did not often communicate with. The warning system was in effect when an email had been received and was, therefore, after the technical solutions pre-stage. This has a negligible effect on the stages in the model since the warning system would be in-twined with the pre-stage and stage 1. Thus, the pre-stage and stage 1 have a closer connection than previously anticipated in the preliminary model. This should be mentioned because discovering this technical solution revealed that the stages are more fluid and have a closer connection to each other than first thought. The model should represent this fluidity to show that traversal in the model is not locked to one path, as is paramount in stage theories.

5.1.3 First interaction with phishing (Stage 1)

We choose to call initial contact the first stage because this is the first stage involving the human element. Considering the human-centric approach to phishing, we found it suitable to have this point in the model be the first stage and the technical part of the model as a pre-stage. The first stage was named initial contact based on the same reasoning of why it is the first stage, namely that this is the first point of contact between a phishing attack and a human. The stage constitutes three main consecutive activities. Namely, delivery, ignore, and explore. Delivery exists in the borderland between the previous stage and this one, while the other activities are firmly placed under stage 1.

Delivery of phishing email

During our study, we found out that the placement of the delivery activity in our preliminary model does not necessarily reflect what we found out about the phishing process. The border between the pre-stage and delivery in stage 1 is more flexible than we initially thought, as mentioned in section sub-section: technical solutions. From literature such as Khonji et al.

(2013), we predominantly found that the pre-stage technical solutions only constituted the technical countermeasures activity. However, with findings related to warnings during the delivery activity, it could be argued that the pre-stage partially constitutes the delivery activity. Since not all emails are filtered out during the previous stage, it supports the inclusion of subsequent stages, including the delivery activity. Thus we place the delivery activity in the borderland between the pre-stage and stage 1. Had technical solutions been flawless, there would not have been a need to research the stages we go through when exposed to phishing attacks.

Although Wang et al. (2012); Williams et al. (2018); Yeboah-Boateng and Amanor (2014) mentions several forms of receiving phishing messages, we predominantly found the mention of emails and some supplementary mentions of SMiShing. However, everything concerning the previous, current, and coming stages and constituent activities still applies regardless of the delivery method. Ultimately the warnings received in the previous stage and during the delivery impact the following activities when we explore the phishing message.

Ignoring the attempt

The ignore activity was a stage that initially would be the path for the individuals who failed to report or do any action which could set themselves in danger. It is built on signal detection theory (Pastore and Scheirer, 1974) and protection motivation theory (Rogers, 1975), where the individual would be able to distinguish discrepancies in the phishing attempt but not feel vulnerable from the attack and therefore not be motivated to protect them self or others. In the findings, we discovered that individuals would actively ignore emails as they would not see any negative consequences. The organization could even have active policies stating that individuals should report untrustworthy emails, which would still not motivate individuals to report the email.

A phishing attempt can be ignored when the attempt has gone through the technical solutions and has been delivered to the individual. However, some individuals will not explore the email before they ignore it. This means that some individuals would miss legit communication but also miss out on phishing attempts, and an individual can choose to ignore the email throughout the process.

This validates that the ignoring activity is present in the model and its placement, but it also shows that individuals need to have the motivation to report by either making them feel that reporting makes them more protected or showing the consequence of ignoring the phishing attempt. Nguyen et al. (2023) mention multiple awareness training methods that could motivate them to report the phishing attempt but also by reminding them of the threat of phishing and the consequences a single mouse click can have for the organization.

The way we explore emails

Through the findings, two distinct processing routes were discovered to be utilized. They align with what we know from existing literature, specifically regarding HSM (Vishwanath et al., 2018; Luo et al., 2013) and ELM (Harrison et al., 2016; Vishwanath et al., 2011). The chosen processing route significantly influences the initial contact stage, particularly the exploring activity. Additionally, the mode of information processing used impacts the ability to assess the content of an email and thus making the selection of processing route crucial to prevent phishing attacks. We found that individuals predominantly relied on the heuristic processing route. An individual's intuition plays a crucial part when exploring or assessing the content of a phishing attempt. Parallels can be drawn to both the heuristic processing route in HSM and the peripheral processing route in ELM. Additionally, when suspicion arose, the individual would further explore the email's content for potential leakage cues and consequently recognize it as a phishing attempt. In other words, when suspicion arose, the individual would switch to the systematic processing route in HSM and the central processing route in ELM to allocate extra mental focus and cognitive resources to explore the content of the email further.

As Harrison et al. (2016) mentioned, the choice or switch between the two routes occurs when the individual connects the elements of the explored email and prior knowledge and experience. We found that this connection occurs when the individual becomes suspicious, triggering a switch in processing mode. This switch predominately keeps us from harm's way regarding phishing since Vishwanath et al. (2011) discovered that we get phished for two reasons. First, we do not adequately process the information in an email but instead rely on simple cues. The second reason is that habitual patterns of media users tend to trigger automatic responses to relevant-looking emails. Switching processing mode can circumvent these two main reasons and lower our susceptibility.

A way to avoid raising suspicion and keeping us in the desired processing route for the attacker is to create highly specific phishing messages. This can be inferred from literature such as Vishwanath et al. (2018) and the two main reasons we get phished presented previously. Looking at the first reason infers that having a highly specific phishing message strengthens the fact that we rely on simple cues keeping us in the desired processing route, i.e., the heuristic processing route. One finding related to the second reason is that if there was a situation where the message was highly specific. For example, had someone recently sent something to Verizon customer support, they expect to receive a reply. If that "reply" happens to be a phishing email pretending to be Verizon customer support, it would not set off any alarms and keep the target in the heuristic processing route. Highly specific messages could also align with what Moody et al. (2017) argue about the content of an email message. Moody et al. (2017) mainly presented different techniques' impact on predicting user compliance. These techniques range from liking the perceived sender, reciprocity, social proof, consistency, authority, and scarcity. Threat actors could utilize this knowledge, especially the consistency part, to create highly specific messages consistent with what we expected in the first place. Being aware of this and in what stage it can affect us could allow for the creation of training programs that emphasize the need to be critical and to work on lowering the mental resources needed to shift processing routes to the systematic one. The different types of training mentioned by Nguyen et al. (2023) and Driskell et al. (1992), such as rule-based training, mindfulness, and over-learning, can help as non-technical solutions to lower the impact of phishing attacks. Providing employees with awareness training can reduce the mental resources needed to connect elements of the phishing message with prior knowledge and thus shift processing route.

The literature tells us that individuals with a higher level of knowledge in recognizing phishing attempts tend to rely more on systematic and central processing routes, requiring fewer cognitive resources to evaluate the content of a message (Vishwanath et al., 2011, 2018; Luo et al., 2013; Harrison et al., 2016). However, an intriguing case emerged from our findings. Individuals who had received comprehensive training and exposure to regular phishing tests perceived their knowledge as substantial and thus that minimal cognitive resources were necessary to assess the content of an email. Consistently sending phishing tests might make people choose the systematic processing route more frequently. Surprisingly some individuals who had received this kind of training still fell victim to phishing tests. These incidents highlight that even individuals equipped with extensive knowledge can be susceptible to phishing attacks if their intuitive judgments fail them, or in other words, they never make the connection between the elements and prior knowledge, i.e., get stuck in the heuristic processing route. It serves as a compelling reminder that one should never underestimate the potential vulnerability to phishing, regardless of their level of knowledge. Vigilance and caution must be exercised consistently, as even the most informed individuals can become targets of deception, although more infrequently than uninformed individuals. Recognizing and responding appropriately to suspicious emails relies heavily on the interplay between these two processing routes.

As mentioned in section 5.1.2 Hindering phishing, some tools give us warnings when we receive emails that could be malicious. These warnings alert us during the delivery activity and impact how we act in the subsequent stage and activities when exploring the content of the message. As mentioned in the Delivery 4.3.1, individuals rely on technological tools to give them warnings and alert them. Our findings entail that these warnings automatically place individuals in the systematic processing route since they know the emails could be malicious. Having such tools to warn us is beneficial since it triggers a move to the systematic processing route regardless of whether or not a connection between elements of the message and prior knowledge and experience would have happened. Since we are more likely to identify a phishing attempt when following the systematic processing route, it is vital to understand the interplay between the two different processing routes, their implications for phishing susceptibility, and how we can trigger the use of the systematic route. 2

5.1.4 Response to phishing (Stage 2)

The second stage of the model consists of actions an individual could perform when responding to a phishing message. Following one path leads to interaction with the phishing attempt, which leads to what we know from the literature as PFM and its stages. On the other hand, the other path leads to reporting the phishing attempt so that the technical countermeasures can learn from the reported phishing attempt.

Awareness and knowledge affect our susceptibility

The literature emphasizes quite clearly that knowledge and prior experience are attributes that affect our susceptibility (Abbasi et al., 2021; Burns et al., 2013; Harrison et al., 2016; Moody et al., 2017; Qabajeh et al., 2018; Vishwanath et al., 2011). Throughout our findings, we found evidence that supported this emphasis. When individuals are aware of the tactics employed by threat actors, they are more likely to exercise caution and make informed decisions when encountering suspicious emails or messages. For example, understanding that legitimate organizations like The Norwegian Tax Administration do not request sensitive information via email or that the email contains links can prompt individuals to refrain from clicking on suspicious links and instead visit the website directly. Since it can act as a form of leakage cue in addition to the common leakage cues mentioned by Butavicius et al. (2022); Parsons et al. (2016); Canfield et al. (2016).

Knowledge of the services individuals use also plays a crucial role. For example, an email from an unfamiliar source or a service you do not utilize is a red flag, alerting you to a possible phishing attempt. In addition to this being aware of what the company's policies are could also play a crucial part in identifying phishing attempts. For instance, knowing that the policy does not include a standardized password manager will make you alert if you receive an email from a password manager asking to update it across the organization. Additionally, consciously entering the URL of a website instead of clicking on provided links can be an effective preventive measure against phishing attacks and may hinder the move from the exploring activity to the interaction activity, regardless of whether the attempt is immediately identified. In essence, the more informed and aware individuals are about phishing, the better equipped they become to protect themselves and minimize the risk of falling victim to such attacks.

Potentially dangerous actions

In the findings, empirical evidence supported what we had researched during our literature review, namely the support of the interaction activity. Abbasi et al. (2021) and Burns et al. (2013) explicitly mentioned the action of clicking a link, while Abbasi et al. (2021) is indirectly mentioned as a prerequisite for the visit stage. In our findings, under section 4.4.2, the activity of clicking a link was mentioned. The typical explanation from the literature and our findings were that the link redirected an individual to a web page that tried to extract personal information. However, We found that identifying a phishing email could happen during the interaction activity before arriving at the phishing website. Should the potential victim not recognize it as a phishing attempt during the exploring activity and click the link, there is still one thing that can alert them, namely by the URL kicking, or in other words, by being redirected. Even though movement between the stages might seem rigid and linear, they are quite fluid. It is possible to revert movement anytime should it be recognized as phishing. For instance, once the URL starts kicking, it can halt the movement between the interaction activity and the browsing activity and move back to the report or ignore activity, depending on an individual's training.

Interestingly we found that clicking a link is harmful in more than one way and that individuals do not have to venture further into the subsequent stages to cause harm. Even though the movement through the stages halts before reaching the dangerous stage 3, some harm has been done. The findings explained that once an individual interacts with the phishing message, the threat actor would know that the email belonged to someone susceptible, and thus some damage would have already been done. By playing the long game, they might have failed this time, but further attempts can be targeted to those the threat actor has identified as susceptible in previous attempts. The individual in question would have to be vigilant in the following months.

The route to reporting

Reporting in the preliminary model was based on the anti-phishing life cycle (Khonji et al., 2013) in which an attack was detected through user awareness or technical solutions. The reporting activity was therefore modeled to show how detection works with user awareness. The findings validated that individuals talked about their experience with phishing and what led them to report the phishing attempt. However, it was discovered that there were two channels in which an individual would report, the official channel, which benefited the technical solutions, and an unofficial channel, where the individual would inform others either next to them in real life or in a chat group.

The findings enlightened us about how individuals reported in the official channel when they followed the life-cycle of the anti-phishing (Khonji et al., 2013) by detecting the phishing attempt and letting the security department in the organization choose their next approach. However, some individuals believed that the organization would apply corrective actions. This stems from their belief that the organization would put the email information into a technical countermeasure that would filter or block the email for the rest of the company. Their belief was backed up by the literature on technical solutions and our findings on what happens when they report the email. This validates that the official reporting system strengthens the technical solutions' resistance and has a positive feedback loop to the technical solutions pre-stage.

5.1.5 Consistency between literature and findings (Stage 3)

The last stage of the model is primarily influenced by Abbasi et al. (2021) work on the PFM. The previous stages explain what results in individuals reaching the first stage in

PFM, namely, visit. In contrast, the third stage in our model follows the same path as the three later stages in PFM browse, consider legitimate, and intend to transact. We focused our research on the IT consultant sector, and considering our sample size, it might be challenging to explain why this stage should be included. However, we found that what we know from the literature by Abbasi et al. (2021) is consistent with our findings, supporting that this is a crucial stage to include in the model.

Similarity between stages

We found similarities between the activities in stage 3 and the previous stages. The main similarities are between the exploring activity in stage 1 and the browsing activity in stage 3. The browsing activity uses many of the same concepts as the explore activity. The explore activity has concepts such as leakage cues and how we process information. Interestingly we can find the same concepts in the browsing activity. The reason for this is that the act of exploring a phishing message is quite similar to the act of browsing a bogus website. The potential victim has to explore the bogus website and look for leakage cues before deciding whether the site is legitimate. Thus, how we process the information on the given site will also impact this decision (Vishwanath et al., 2011, 2018; Luo et al., 2013; Harrison et al., 2016). Similarly, the consider legitimate activity can be drawn into the explore activity since such a consideration of whether to interact or report the phishing attempt has to be made.

The same argument about highly specific messages can be made when discussing the consider legitimate activity as was made when discussing the explore activity. Should the potential victim have decided to interact with the "reply" you got from those pretending to be Verizon customer support, they would most likely be in the heuristic processing route since they already expected to be contacted by Verizon. Thus, they likely consider the website legitimate and intend to transact with it. Had they not expected to hear from Verizon, it would be far more likely that they either ignored the phishing attempt or reported it.

5.2 Practical implications

The Practical Implications section of the discussion in this thesis aims to put the research findings into actionable insights and real-world applications. By doing this, we aim to shed light on how the research outcome can be utilized to address practical challenges and inform decision-making processes. This section delves into the potential implications for organizations, policymakers, practitioners, and other stakeholders.

5.2.1 A little help from a friend

In 5.1.4, the theoretical implications of the model were discussed. However, when we found that some individuals utilized an unofficial reporting system, some practical implications followed. The unofficial reporting system took the form in which an individual would communicate with their colleagues if the attempt were phishing, either through talking with them or by communicating the threat in a chat group. Our findings expanded this by mentioning that some individuals would talk with other colleagues to confirm if they had received the phishing attempt.

The interesting point was that some individuals would inform their colleagues in some form, even after confirming that the communication was a phishing attempt. This might be because they feel that the threat has been neutralized when they engaged their colleagues in the process and that confirming the phishing attempt has given them a feeling of contributing to protecting the organization. However, for the organization, this unofficial system of reporting only benefits some parts of the organization. The unofficial systems protect the individuals who have been made aware of the phishing attempt but not every department, and it does not necessarily make the organization's security department aware of the threat.

The unofficial system can strengthen the official system if the individual reports the phishing attempt in the official system as well as inform their colleagues about the threat. However, they need to be educated about the threat that phishing can cause and why it benefits them to report the phishing attempt. If individuals understand the consequence not reporting has on both them and the organization, they might be motivated to report the phishing attempt. The individual could also feel motivated to teach the consequence to the people around them or inform them to report the email. However, The unofficial system still has the benefit that it helps some individuals in the organization, and an open environment could help increase this form of reporting.

An environment where individuals talk with each other could benefit an organization's security by creating a more aware environment toward potential phishing attempts. If individuals can discuss the potential threat and come to a collective conclusion, then it would benefit the whole environment, and potential blame would be put on the collective, not a single individual. However, in an environment where individuals were separated from each other and could not discuss potential threats, an unofficial system would not flourish, and this could either cause a higher amount of reporting but also cause a more considerable amount of ignoring.

5.2.2 Utilizing knowledge

As mentioned in section 5.1, we process information following one of two routes. The choice of processing route ultimately impacts our susceptibility to phishing attacks. However, it might not be a conscious choice but rather an unconscious decision to switch from the heuristic processing route to the systematic processing route once a connection has been made with the elements of the phishing message, i.e., leakage cues and the existing knowledge possessed by an individual. The critical part here is existing knowledge. Since knowledge is not finite and continues to evolve, so can a person's knowledge if proper training is implemented. Organizations could conduct systematic training targeted to enhancing employees phishing knowledge and awareness in order to bridge the gap between existing knowledge and these elements so that a connection can be made, thus triggering this mentioned switch. By having a comprehensive understanding of these processing routes, organizations can better promote cybersecurity practices and enhance their resilience against phishing attacks.

We found that older individuals were more prone to report phishing attempts than younger individuals, who mostly ignored phishing attempts. The training previously mentioned could be targeted to younger employees to build their knowledge further to identify phishing and report attempts. Increasing the number of employees who report phishing attempts instead of ignoring them would benefit the entire organization.

To supplement the training, the consistent use of phishing tests could help employees utilize their knowledge and further enhance it. For example, one of our findings suggests that working in an environment where phishing tests were regularly sent out could make individuals finding the switch from the heuristic route to the systematic route easier. In other words, it required less cognitive resources to make the switch. This is what organizations could benefit from having this understanding.

5.2.3 Susceptible targets

As mentioned in section 5.1.4 our findings indicate that clicking on a link can have more harmful consequences than initially anticipated. By clicking on a link, individuals can attract the attention of threat actors and become vulnerable to subsequent phishing attacks. They know this person is susceptible to being deceived by a phishing attack, having already gone so far as to interact with a phishing attempt. Further attempts could utilize more specific messages hoping that one strikes home. Having this knowledge, however, companies can allocate further resources to susceptible employees from the attacker's point of view. Should a link be clicked, the individual could alert the IT department, assuming proper training and knowledge to do so, and extra security measures could be put in place for the employee in question. Depending on how many have clicked the link, this might be a cost-effective way to hamper threat actors. Based on insights from existing literature and our findings, it is observed that a majority of employees in the IT sector are less prone to interact with phishing messages and click on links, making it an enticing countermeasure for companies operating in this industry.

5.3 Limitations and opportunities for further research

This section will present the limitations of our thesis and explore potential hypotheses found in the thesis that could be further explored. In addition, it will be used to show potential research gaps that have been found, but because of the thesis's scope and focus, these gaps have not been filled..

5.3.1 Limitations

It is essential to acknowledge that this thesis has certain limitations. Firstly the sample size used in this study restricted the capability of conceptualizing the findings in broader terms and with a larger population. Additionally, the over-representation of men among the interviewees limited the understanding of how the phishing process manifests across diverse demographic groups. While efforts were made to ensure the research's validity and reliability, having a more extensive and diverse sample would have provided a broader perspective and increased the robustness of the thesis.

Another limitation pertains to the narrow focus on the IT sector. As a result, it may not fully capture the experiences and perspectives of individuals from other industries and sectors. Thus, the findings lack comprehensive applicability and may not fully represent the nuances of the phishing process across different sectors.

These limitations may provide opportunities for future research to address these gaps and broaden the scope of inquiry. By expanding the sample size, ensuring a diverse representation, and including participants from various sectors, future studies can provide a more comprehensive understanding of the phenomenon of phishing from the victim's perspective. Unfortunately, given the time limit on this thesis and the resources at hand, we could not pursue to fill these gaps nor expand our scope to address other exciting concepts, such as exploring and validating the factors impacting us during each stage and their constituent activities.

5.3.2 Validating the model on a larger scale

The model in this thesis is not necessarily complete, as the scope of the thesis has been focused on the IT sector, and the individuals interviewed were aware that they had been exposed to phishing. The model could be validated on a larger scale where individuals from multiple sectors are included, but also individuals who do not know if they have been exposed to phishing. This could be done by having a more extensive qualitative study and conducting interviews in multiple sectors or by doing a more extensive phishing test in which the individuals have been exposed to phishing without knowing. The last approach, however, raises multiple ethical dilemmas, as the individual would not know why they are participating and if they would have done something wrong.

5.3.3 Further study of Stage 3 Transaction

In our thesis, the foundation of stage 3 Transaction is primarily built upon the research conducted by Abbasi et al. (2021) and their work on the phishing funnel model. Although our primary focus has been to understand the stages individuals go through leading up to the phishing funnel model, we recognized the necessity of including the funnel stages to obtain a holistic view.

Since our study specifically targeted the IT sector, we engaged in interviews with participants who guided us through a hypothetical phishing attack, including stage 3 and its activities. This approach allowed us to gather valuable insights within the context of our study. However, to further enhance the understanding of this stage and its constituent activities, future studies could expand upon this by expanding their scope, incorporating multiple sectors, and employing a larger sample size. Such studies would contribute to a broader exploration of the importance and implications associated with this stage.

5.3.4 Phishing in an open vs closed environment

From our findings, an interesting question arose about the potential phishing in an open work environment compared to a closed environment and the security benefits this might have for an organization. As mentioned in section 5.2.1 the findings suggested that an unofficial reporting system was in place. This system used the social groups formed in an organization to discuss potential phishing attempts that could benefit the organization in a minor way. This, however, is still unknown to which degree an unofficial report system benefits the system and if the benefits would be more substantial in an open work environment compared to a closed work environment. The hypothesis is that an open work environment in which the individuals have gotten awareness training and are free to discuss potential threats would be less susceptible to phishing than a closed work environment in which the individuals are split from their colleagues.

This hypothesis could be studied by looking at work environments, where individuals would repeatably be exposed to phishing but can also be tested by exposing a group of individuals to phishing where one group is exposed to phishing as a group and another group is exposed to phishing as individuals split from each other and exam their actions. Then, to test the strength of the collective, the experiment can be rerun, but this time educate the groups about phishing and its threat.

In addition, identifying the impact of an open work environment on phishing, in contrast to a closed work environment, could be interesting. Several studies mention the effect open work environment has on employees' productivity. Therefore, contrasting the potential cost savings of a phishing attack with productivity loss may lead to some interesting findings.

5.3.5 How different generations report?

During the interviews, a finding that we needed more data to explore was discovered. This finding was that the older individuals participating in the interviews often stated that they reported the phishing attempt, while the younger participants often ignored it. They would, however, more often report the phishing attempt through the unofficial system and spread the information in their chat groups than their older colleagues. There is a hypothesis that the younger generation does not report less than the older generation but does this differently. In addition, examining the unofficial reporting system's impact on phishing and its effectiveness could be of interest.

By addressing these limitations and delving deeper into these points of further research, we can continue to advance our knowledge and understanding of phishing attacks. Ultimately we can enhance our ability to combat and mitigate this ever-evolving cybersecurity threat.

Chapter 6

Conclusion

This study aimed to provide a comprehensive understanding of the phishing phenomenon from the victim's perspective. To achieve this goal, we utilized a theoretical framework based on stage models and leveraged knowledge of existing literature and empirical findings to develop a holistic phishing stage model. The phishing stage model elucidates the overarching stages individuals undergo when exposed to a phishing attack, highlighting the more nuanced activities within these stages. Notably, these activities exhibit a higher level of intricacy than their parent stages. In addition, it is essential to note that the different activities offer individuals various avenues. For instance, interacting with a phishing attempt includes clicking on a fraudulent link or opening a suspicious attachment. Similarly, reporting such attempts can be done through either official or unofficial channels. In this way, individuals possess multiple choices that may not be obvious regarding each activity.

Presenting this model, we offer a valuable framework that effectively explains the stages individuals traverse during the phishing process. This research enhances our understanding of said phenomena by shedding light on phishing attacks from the victim's standpoint. The insight gained from this thesis advances our understanding and offers valuable guidance for developing preventive measures, educational initiatives, training programs, and robust cybersecurity strategies. Furthermore, the model presented in this study serves as a valuable tool for identifying focal points in training efforts, thus enabling organizations to address vulnerabilities and effectively enhance their defenses against phishing attacks.

This thesis also makes a noteworthy contribution to the broader research field by bridging the existing knowledge gap concerning how individuals become victims of phishing attacks. By investigating the phenomena from the victim's perspective, we contribute to a body of knowledge by offering a comprehensive understanding that can inform future studies and initiatives to combat phishing threats.

In conclusion, this study has provided a comprehensive understanding of the phishing phenomenon from the victim's perspective, utilizing a well-structured theoretical framework and incorporating insight from existing literature and empirical findings. Furthermore, the phishing stage model developed in this thesis elucidates the stages and constituent activities individuals undergo when exposed to phishing attacks. Thus it presents a valuable framework for understanding and addressing this pervasive cybersecurity threat.

Bibliography

Ahmed Abbasi, David Dobolyi, Anthony Vance, and Fatemeh Mariam Zahedi. The phishing funnel model: a design artifact to predict user susceptibility to phishing websites. *Information Systems Research*, 32(2):410–436, 2021.

Hossein Abroshan, Jan Devos, Geert Poels, and Eric Laermans. Phishing happens beyond technology: the effects of human behaviors and demographics on each step of a phishing process. *IEEE Access*, 9:44928–44949, 2021.

Steve Alder. Study confirms security awareness training significantly reduces susceptibility to phishing attacks, 2022. URL https://www.hipaajournal.com/study-confirms-security-awareness-training-significantly-reduces-susceptibility-to-

Ali Alsaawi. A critical review of qualitative interviews. *European Journal of Business and Social Sciences*, 3(4), 2014.

Hamza Alshenqeeti. Interviewing as a data collection method: A critical review. *English linguistics research*, 3(1):39–45, 2014.

APWG. 1st quarter 2022 - apwg, a. URL https://docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf.

APWG. 3rd quarter 2022 - docs.apwg.org, b. URL https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf.

APWG. Phishing activity trends report, 4th quarter 2022, 05 2023. URL https://docs.apwg.org/reports/apwg_trends_report_q4_2022.pdf.

Mary B Burns, Alexandra Durcikova, and Jeffrey L Jenkins. What kind of interventions can help users from falling for phishing attempts: A research proposal for examining stage-appropriate interventions. In *2013 46th Hawaii International Conference on System Sciences*, pages 4023–4032. IEEE, 2013.

Marcus Butavicius, Ronnie Taib, and Simon J. Han. Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers Security*, 123:102937, 2022. ISSN 0167-4048. doi: https://doi.org/10.1016/j.cose.2022.102937. URL https://www.sciencedirect.com/science/article/pii/S0167404822003297.

Casey Inez Canfield, Baruch Fischhoff, and Alex Davis. Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors*, 58(8):1158–1172, 2016. doi: 10.1177/0018720816665025. URL https://doi.org/10.1177/0018720816665025. PMID: 27562565.

HU Chih-Pei and Yan-Yi Chang. John w. creswell, research design: Qualitative, quantitative, and mixed methods approaches. *Journal of Social and Administrative Sciences*, 4(2):205–207, 2017.

John W Creswell. The selection of a research design the three types of designs. 2008. URL https://www.sagepub.com/sites/default/files/upm-binaries/22780_Chapter_1.pdf.

Sanchari Das, Christena Nippert-Eng, and L Jean Camp. Evaluating user susceptibility to phishing attacks. *Information & Computer Security*, 30(1):1–18, 2022.

Rachna Dhamija, J Doug Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 581–590, 2006.

James E Driskell, Ruth P Willis, and Carolyn Copper. Effect of overlearning on retention. *Journal of Applied Psychology*, 77(5):615, 1992.

Brynne Harrison, Elena Svetieva, and Arun Vishwanath. Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*, 40(2):265–281, 2016.

Allen C Johnston and Merrill Warkentin. Fear appeals and information security behaviors: An empirical study. *MIS quarterly*, pages 549–566, 2010.

Bonnie Kaplan and Joseph A Maxwell. Qualitative research methods for evaluating computer information systems. *Evaluating the organizational impact of healthcare information systems*, pages 30–55, 2005.

Mahmoud Khonji, Youssef Iraqi, and Andrew Jones. Phishing detection: A literature survey. *IEEE Communications Surveys Tutorials*, 15(4):2091–2121, 2013. doi: 10.1109/SURV.2013.032213.00009.

B. Kitchenham and S. Charters. Guidelines for performing systematic literature reviews in software engineering. Technical report, Technical report, ver. 2.3 ebse technical report. ebse, 2007.

Ponnurangam Kumaraguru, Yong Rhee, Steve Sheng, Sharique Hasan, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, pages 70–81, 2007.

Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.

LockheedMartin. The cyber kill chain, 2023. URL https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Xin Robert Luo, Wei Zhang, Stephen Burd, and Alessandro Seazzu. Investigating phishing victimization with the heuristic–systematic model: A theoretical framework and an exploration. *Computers & Security*, 38:28–38, 2013.

Jaclyn Martin, Chad Dubé, and Michael D Coovert. Signal detection theory (sdt) is effective for modeling user behavior toward phishing and spear-phishing attacks. *Human factors*, 60(8):1179–1191, 2018.

Michael JA Miranda. Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, 14(2):5–10, 2018.

Gregory D Moody, Dennis F Galletta, and Brian Kimball Dunn. Which phish get caught? an exploratory study of individuals susceptibility to phishing. *European Journal of Information Systems*, 26:564–584, 2017.

Michael D Myers and David Avison. *Qualitative research in information systems: a reader*. Sage, 2002.

Christopher Nguyen, Matthew Jensen, and Eric Day. Learning not to take the bait: a longitudinal examination of digital training methods and overlearning on phishing susceptibility. *European Journal of Information Systems*, 32(2):238–262, 2023. doi: 10.1080/0960085X.2021.1931494. URL https://doi.org/10.1080/0960085X.2021.1931494.

Briony J Oates, Marie Griffiths, and Rachel McLean. *Researching information systems and computing*. Sage, 2022.

Kathryn Parsons, Marcus Butavicius, Malcolm Pattinson, Dragana Calic, Agata Mccormac, and Cate Jerram. Do users focus on the correct cues to differentiate between phishing and genuine emails?, 2016. URL https://arxiv.org/abs/1605.04717.

RE Pastore and CJ Scheirer. Signal detection theory: Considerations for general application. *Psychological Bulletin*, 81(12):945, 1974.

Richard E Petty, John T Cacioppo, Richard E Petty, and John T Cacioppo. *The elaboration likelihood model of persuasion*. Springer, 1986.

proofpoint. State of the phish, 2023. URL https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2023.pdf.

Issa Qabajeh, Fadi Thabtah, and Francisco Chiclana. A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review*, 29:44–55, 2018.

Marc Rader and Shawon Rahman. Exploring historical and emerging phishing techniques and mitigating the associated security risks. *International Journal of Network Security Its Applications*, 5, 11 2015. doi: 10.5121/ijnsa.2013.5402.

Ronald W Rogers. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, 91(1):93–114, 1975.

Suprateek Sarker, Xiao Xiao, Tanya Beaulieu, and Allen S Lee. Learning from first-generation qualitative approaches in the is discipline: An evolutionary view and some implications for authors and evaluators (part 1/2). *Journal of the Association for Information Systems*, 19(8):1, 2018.

Anjum N. Shaikh, Antesar M. Shabut, and M.A. Hossain. A literature review on phishing crime, prevention review and investigation of gaps. In *2016 10th International Conference on Software, Knowledge, Information Management Applications (SKIMA)*, pages 9–15, 2016. doi: 10.1109/SKIMA.2016.7916190.

Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 373–382, 2010.

Sikt. About sikt - norwegian agency for shared services in education and research, 2023. URL https://sikt.no/en/about-sikt.

Wael Soliman and Virpi Kristiina Tuunainen. A tale of two frames: Exploring the role of framing in the use discontinuance of volitionally adopted technology. *Information Systems Journal*, 32(3):473–519, 2022.

David R Thomas. A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation*, 27(2):237–246, 2006.

Aggeliki Tsohou, Mikko Siponen, and Mike Newman. How does information technology-based service degradation influence consumers' use of services? an information technology-based service degradation decision theory. *Journal of Information Technology*, 35(1):2–24, 2020.

Andrew H Van de Ven and Rhonda M Engleman. Event-and outcome-driven explanations of entrepreneurship. *Journal of Business Venturing*, 19(3):343–358, 2004.

Arun Vishwanath, Tejaswini Herath, Rui Chen, Jingguo Wang, and H Raghav Rao. Why do people get phished? testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3):576–586, 2011.

Arun Vishwanath, Brynne Harrison, and Yu Jie Ng. Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 45(8):1146–1166, 2018.

Jingguo Wang, Tejaswini Herath, Rui Chen, Arun Vishwanath, and H. Raghav Rao. Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, 55(4):345–362, 2012. doi: 10.1109/TPC.2012.2208392.

Jane Webster and Richard T Watson. Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, pages xiii–xxiii, 2002.

Neil D Weinstein, Alexander J Rothman, and Stephen R Sutton. Stage theories of health behavior: conceptual and methodological issues. *Health psychology*, 17(3):290, 1998.

Emma J. Williams, Joanne Hinds, and Adam N. Joinson. Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120:1–13, 2018. ISSN 1071-5819. doi: https://doi.org/10.1016/j.ijhcs.2018.06.004. URL https://www.sciencedirect.com/science/article/pii/S1071581918303628.

Michael Workman. Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American society for information science and technology*, 59(4):662–674, 2008.

Ryan T Wright, Matthew L Jensen, Jason Bennett Thatcher, Michael Dinger, and Kent Marett. Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. *Information systems research*, 25(2):385–400, 2014.

Yu Xiao and Maria Watson. Guidance on conducting a systematic literature review. *Journal of planning education and research*, 39(1):93–112, 2019.

Ezer Osei Yeboah-Boateng and Priscilla Mateko Amanor. Phishing, smishing & vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, 5(4):297–307, 2014.

Appendix A

Interview questions

Del 1: Generell info om intervjuobjektet som bakgrunn og erfaringer

1. Hvor gammel er du?
2. Hvilken utdannelse er det du har?
3. Hvilken stilling og arbeidserfaring har du?
4. Hvor teknisk god vil du selv si du er?
5. Har du tillit til at samfunnet, institusjoner, arbeidsplasser og nettsider skal ta vare på din sikkerhet?
6. Hvor stor risiko tror du at det er ved bruken av pc, internett og andre applikasjoner?
    (a) Endrer denne risikoen seg i jobbsammenheng?

Del 2: Phishing og phishing prosessen

1. Hva vet du om phishing?
2. Hva er dine erfaringer med phishing?
3. Hvordan kan man oppdage at en e-post er phishing?
4. Fortell oss om tankegangen din fra du åpnet en phishing e-posten til du gjorde en handling?
    (a) Hvor lang tid brukte du på denne tankeprosessen?
5. Har du hatt gjennom din arbeidsplass eller på eget initiativ kursing eller trening som har vært rettet mot phishing?

Del 3: Feedback

1. Har du noen konstruktiv tilbakemelding til hvordan vi utførte intervjuet?

Appendix B

Interview guide

Takk for at du deltar i dette intervjuet med oss. Hensikten med dette intervjuet er å undersøke stegene man går igjennom når man blir utsatt for et phishing angrep. Målet med intervjuet er å forstå hvordan man tenker og hva man gjør når man blir utsatt for phishing, for å potensielt etablere en felles konsensus for stegene man tar basert på svarene dine og den kunnskapen vi har opparbeidet oss gjennom litteraturgjennomgangen. Vi vil derfor sammenligne svarene dine med andre intervjuobjekter for å utvikle stadiene vi tror man går igjennom. Intervjuet vil derfor forsøke å utvide den forståelsen vi har for stadiene i phishing prosessen, samt stille spørsmål for å utfylle eventuelle mangler vi har i vår kunnskap.

Dette intervjuet er anonymt. Vi vil IKKE skrive personlig informasjon om deg. Eventuelle personlige opplysninger vil ikke bli transkribert eller lagt til i dokumentet, og alle opptak vil bli slettet ved slutten av hovedleveransen, beregnet dato: 02.06.2023. Du står fritt til å nekte å svare på spørsmål uten å gi grunnlag for dette. Dette intervjuet og informasjonen innhentet fra det, vil bli brukt i masteroppgaven "Holistic phishing stage model: How do people get phished?" og ved å delta gir du samtykke til studentene ved UiA under Master: Cybersikkerhet ledelse: Filip Zeitz Schou Grøtterud og Kristian Bjurholt Rein, å bruke intervjuet og ta det opp i masteroppgaven deres. Det er kun Filip Zeitz Schou Grøtterud og Kristian Bjurholt Rein som behandler dataene fra intervjuet før de blir anonymisert.

Intervjuet er semistrukturert og vil stille spørsmål om phishing og phishing prosessen for å kunne forstå stadiene individer går igjennom når de blir utsatt for phishing å dermed kunne lage en helhetlig modell som forklarer prosessen og kan bevisstgjøre trusselen av phishing.

Det er ønskelig at vi klarer å holde oss litt innenfor temaet som diskuteres med en viss vekt på å være kort og konsis

Estimert tid for dette intervjuet er 20-30 minutter.

Del 1: Generell info om intervjuobjektet som bakgrunn og erfaringer

1. Hvor gammel er du?
2. Hvilken utdannelse er det du har?
3. Hvilken stilling og arbeidserfaring har du?
4. Hvor teknisk god vil du selv si du er?
5. Har du tillit til at samfunnet, institusjoner, arbeidsplasser og nettsider skal ta vare på din sikkerhet?
6. Hvor stor risiko tror du at det er ved bruken av pc, internett og andre applikasjoner?
   (a) Endrer denne risikoen seg i jobbsammenheng?

Del 2: Phishing og phishing prosessen

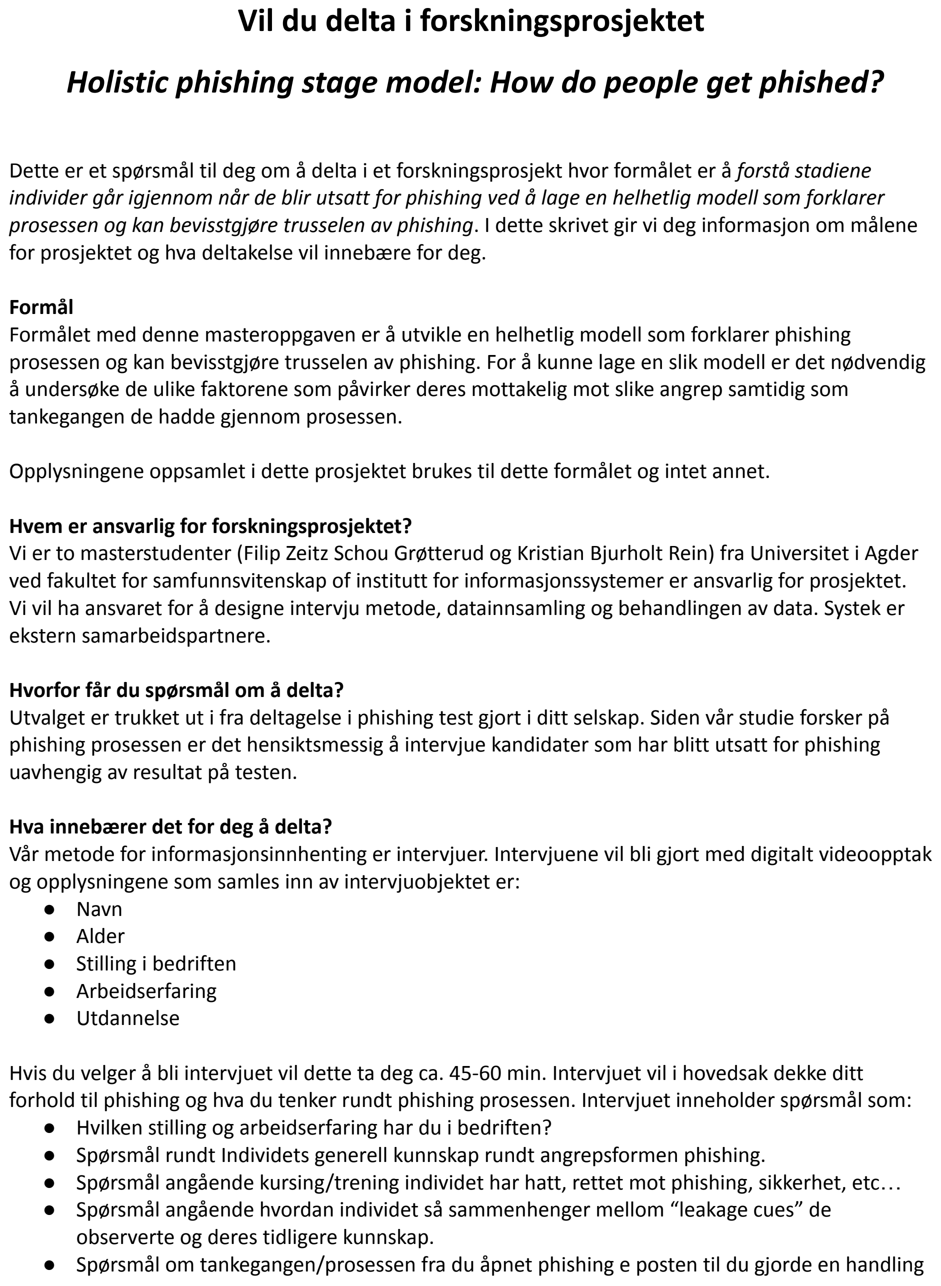
1. Hva vet du om phishing?
2. Hva er dine erfaringer med phishing?
3. Hvordan kan man oppdage at en e-post er phishing?
4. Fortell oss om tankegangen din fra du åpnet en phishing e-posten til du gjorde en handling?
   (a) Hvor lang tid brukte du på denne tankeprosessen?
5. Har du hatt gjennom din arbeidsplass eller på eget initiativ kursing eller trening som har vært rettet mot phishing?

Del 3: Feedback

1. Har du noen konstruktiv tilbakemelding til hvordan vi utførte intervjuet?

Appendix C

Consent form



Vil du delta i forskningsprosjektet

Holistic phishing stage model: How do people get phished?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å *forstå stadiene individer går igjennom når de blir utsatt for phishing ved å lage en helhetlig modell som forklarer prosessen og kan bevisstgjøre trusselen av phishing*. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Formålet med denne masteroppgaven er å utvikle en helhetlig modell som forklarer phishing prosessen og kan bevisstgjøre trusselen av phishing. For å kunne lage en slik modell er det nødvendig å undersøke de ulike faktorene som påvirker deres mottakelig mot slike angrep samtidig som tankegangen de hadde gjennom prosessen.

Opplysningene oppsamlet i dette prosjektet brukes til dette formålet og intet annet.

Hvem er ansvarlig for forskningsprosjektet?
Vi er to masterstudenter (Filip Zeitz Schou Grøtterud og Kristian Bjurholt Rein) fra Universitet i Agder ved fakultet for samfunnsvitenskap of institutt for informasjonssystemer er ansvarlig for prosjektet. Vi vil ha ansvaret for å designe intervju metode, datainnsamling og behandlingen av data. Systek er ekstern samarbeidspartnere.

Hvorfor får du spørsmål om å delta?
Utvalget er trukket ut i fra deltagelse i phishing test gjort i ditt selskap. Siden vår studie forsker på phishing prosessen er det hensiktsmessig å intervjue kandidater som har blitt utsatt for phishing uavhengig av resultat på testen.

Hva innebærer det for deg å delta?
Vår metode for informasjonsinnhenting er intervjuer. Intervjuene vil bli gjort med digitalt videoopptak og opplysningene som samles inn av intervjuobjektet er:

- Navn
- Alder
- Stilling i bedriften
- Arbeidserfaring
- Utdannelse

Hvis du velger å bli intervjuet vil dette ta deg ca. 45-60 min. Intervjuet vil i hovedsak dekke ditt forhold til phishing og hva du tenker rundt phishing prosessen. Intervjuet inneholder spørsmål som:

- Hvilken stilling og arbeidserfaring har du i bedriften?
- Spørsmål rundt Individets generell kunnskap rundt angrepsformen phishing.
- Spørsmål angående kursing/trening individet har hatt, rettet mot phishing, sikkerhet, etc…
- Spørsmål angående hvordan individet så sammenhenger mellom "leakage cues" de observerte og deres tidligere kunnskap.
- Spørsmål om tankegangen/prosessen fra du åpnet phishing e posten til du gjorde en handling

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Kun behandlingsansvarlige Filip Zeitz Schou Grøtterud og Kristian Bjurholt Rein vil ha tilgang til dine opplysninger.
- Kun behandlingsansvarlige Filip Zeitz Schou Grøtterud og Kristian Bjurholt Rein vil samle inn, bearbeide og lagre data.
- Tiltak for at ingen uvedkommende får tilgang til personopplysningene dine inkluderer
    - Navn og annen identifiserbar informasjon vil bli anonymisert og vil kun bli gjengitt som stilling.
    - Bedriften vil bli anonymisert.
    - Dataene vil bli lagret på en kryptert forskningsserver med to-faktor autentisering.

Deltakere vil ikke kunne gjenkjennes i publikasjon. Deltakere vil anonymiseres og refereres til som intervjuobjektet eller f.eks. stilling dersom det er hensiktsmessig.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?
Prosjektet vil etter planen avsluttes 2.juni 2023 og alt av oppbevarte data slettes fullstendig fra alle medier etter sensur.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Filip Zeitz Schou Grøtterud og Kristian Bjurholt Rein har Sikt – Kunnskapssektorens tjenesteleverandør vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- Institutt for informasjonssystemer ved Filip Zeitz Schou Grøtterud fzgrotteru@uia.no og Kristian Bjurholt Rein krisbr18@student.uia.no og/eller veileder Wael Anwar Abdel Aziz Soliman wael.soliman@uia.no ved Institutt for informasjonssystemer
- Vårt personvernombud: Rådgiver/Personvernombud ved institutt for informasjonssystemer: Ina Danielsen in.danielsen@uia.no +47 452 54 401

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via:

- Epost: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Med vennlig hilsen

Filip Zeitz Schou Grøtterud	*Kristian Bjurholt Rein*
filip Zeitz Schou Grøtterud	Rein

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *[sett inn tittel]*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju
- at Filip Zeitz Schou Grøtterud og Kristian Bjurholt Rein kan bruke opplysninger om meg i prosjektet

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

----

(Signert av prosjektdeltaker, dato)