Catch the Phish: A Study on Decision-Making and Reporting Behavior for Phishing Attacks

Master Thesis

Robin Bahl

Catch the Phish: A Study on Decision-Making and Reporting Behavior for Phishing Attacks

Master thesis submitted to Delft University of Technology in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

IN

MANAGEMENT OF TECHNOLOGY

Faculty of Technology, Policy and Management

BY

ROBIN BAHL
Student Number: 5481481

To be defended in public on August 17th, 2023

Graduation Committee

Chairperson	:	Prof. dr. Michel van Eeten	The Organization & Governance Section (O&G
First Supervisor	:	Prof. dr. Simon Parkin	The Organization & Governance Section (O&G)
Second Supervisor	:	Prof. dr. Jenny Lieu	The Organization & Governance Section (O&G)
External Supervisor	:	Rick Punt	Security & Privacy Awareness Consultant (ICT)

TU Delft Delft University of Technology

1 Acknowledgement

As I reflect on this incredible journey of pursuing my masters and completing this thesis, I am filled with immense gratitude for the transformative experience it has been. This process has not only enriched my academic knowledge but has also shaped me as an individual, teaching me valuable lessons in time management, perseverance, and resilience.

I am incredibly grateful for the opportunity to take up courses delivered by Dr. Simon Parkin, including "Economics of Cybersecurity" and "User-Centred Security." These courses not only expanded my knowledge in the field but also sparked a keen interest in the subject matter. Moreover, as my first supervisor, Dr. Simon Parkin's continuous support and guidance have been invaluable. He always took the time to critically reflect on the direction of my thesis, providing detailed and comprehensive feedback that motivated me to continuously improve the quality of this work. My deepest gratitude also extends to Dr. Jenny Lieu, Dr. Michel & Rick Punt for their unwavering support, mentorship, and expertise throughout my research. Their dedication and insightful feedback have played a crucial role in shaping this thesis and enhancing its overall quality. Their encouragement and belief in my abilities have given me the confidence to overcome challenges and achieve milestones.

I extend my sincere thanks to all the participants who willingly shared their time, experiences, and insights during this study. Their valuable contributions and engaging discussions have been at the core of this research. To my family, I cannot thank you enough for being my pillars of strength throughout this journey. Your motivational words have lifted my spirits during moments of doubt, and I am truly grateful for your love and encouragement. A big thank you to my brother, Dhruv, whose calm and composed nature has been a source of reassurance when I faced challenges. His research expertise and unique insights have been a guiding force, helping me overcome any obstacles I encountered.

I am deeply grateful to TU Delft for the invaluable lessons and learning during my academic journey. The university has provided me with ample opportunities for growth, which have significantly contributed to both my professional and personal development. The extensive knowledge and practical skills acquired here have prepared me to confidently tackle future challenges. Lastly, a special thanks to my friends, both at the university and back home, for their constant support throughout this journey.

2 Executive Summary

Phishing attacks are a growing problem worldwide, causing significant losses and damage to individuals, organizations, and governments each year. As attackers use increasingly sophisticated social engineering techniques to deceive their victims into giving away sensitive information or downloading malware, organizations have responded by implementing a range of anti-phishing measures. These measures encompass both technical solutions as well as educational initiatives aimed at promoting reporting and enhancing overall security against phishing attacks. However, despite these efforts, there remains a gap in reporting rates in response to phishing emails. To address this, the present research aims to understand how organizations can foster a reporting culture by exploring the factors that influence reporting behavior and examining the role of infrastructure and support systems in enhancing reporting rates. This educational case study adopts a mixed methods approach, combining perspectives from both the security team and the users. It utilizes qualitative interviews with the security team to gain insights into existing measures and processes and analyze quantitative phishing simulation logs to understand user behavior across different user groups. Subsequently, interviews are conducted with users to gain a deeper understanding of the factors that influence reporting behavior and the role of infrastructure in enhancing reporting.

The organization employs a comprehensive approach to prevent phishing attacks through a multi-layered approach by partnering with different companies that provide a range of solutions and places a strong emphasis on raising awareness among its users through phishing simulation exercises. The organization recognizes that cybersecurity is a team effort and strives to balance security measures with user experience and aims to foster a culture of reporting. The analysis of phishing simulation logs indicate higher susceptibility to phishing attempts among students and faculty, with lower reporting rates observed among students. Furthermore, the analysis of the educational landing page revealed low user engagement, prompting questions about the effectiveness of teaching moments immediately after a user clicks on the link. The reported phishing emails and simulation emails successfully replicated persuasion techniques and targeted impersonation. Peak periods for phishing attempts were also identified, necessitating heightened user vigilance and proactive measures during those times. Among reported phishing emails, attackers commonly employed authority and scarcity as persuasion techniques. The phishing simulation emails effectively replicated these observed techniques, providing users with realistic scenarios to enhance their skills in detecting and responding to sophisticated attacks.

The study utilized the COMB model to identify factors influencing reporting behavior. Under capability, self-efficacy in identifying phishing emails, awareness of consequences, understanding the reporting process, and recognizing the importance of reporting were primary factors affecting reporting behavior. Similarly, within the opportunity, the ease of reporting, time and cost to the user were major factors. Additionally, exposure to phishing emails, timely feedback, and social norms played key roles. Lastly, under motivation, personal work ethic and values, collective responsibility towards colleagues and the organization, personal experiences with phishing, perceived threat level of the email,

and the perceived effectiveness of reporting as an action were identified as factors influencing reporting behavior. Ultimately, fostering a reporting culture necessitates a collaborative effort involving the organization, its users, and technical systems. Users should be encouraged to actively participate in reporting incidents, but the organization must also be mindful of the associated costs and challenges. To achieve this balance, the organization should carefully evaluate the desired reporting level, considering available resources, potential impact of phishing attacks, and the time and effort required from users to report incidents. The organization should ensure a clear and user-friendly reporting process, including a dedicated report button and regular reminders. Communication, transparency, and trust-building are essential for emphasizing the benefits of reporting and providing timely feedback. Training programs play a key role in raising awareness about the consequences of phishing attacks and equipping users with the skills to identify suspicious emails. Incentive programs should be thoughtfully designed to encourage reporting without distracting users from their primary responsibilities. Creating a culture where colleagues support each other can also enhance reporting rates. Leveraging technology, such as implementing notification systems for already reported malicious emails and exploring automated mechanisms to remove flagged emails from users' inboxes, can optimize the reporting process, show appreciation for users' efforts, and reduce reporting burdens. Ultimately, embracing a paradigm shift that recognizes humans as part of the solution, rather than the problem, is crucial in nurturing a reporting culture. These strategies foster a proactive community, actively protecting against phishing attacks and ensuring a secure digital environment.

Contents

List of Tables

List of Figures

3 Introduction

3.1 Background:

In today's digital world, cybersecurity is a pressing concern for both individuals and organizations, as more of our personal and professional lives move online. The rapid advancement of digital technologies has led to significant changes in many industries, with organizations looking for ways to leverage these technologies to improve efficiency, reduce costs, and gain a competitive edge. However, the widespread use of the internet has made individuals more vulnerable to cyber-attacks and sensitive information breaches. Cybercriminals see this as an opportunity to obtain confidential information such as usernames, passwords, bank account information, credit card, or social security numbers, which they can use for criminal activities such as identity theft or fraud. Phishing is one of the most common types of cybercrimes, which involves an attacker impersonating a legitimate institution to trick users into providing personal or financial information(Gupta, Tewari, Jain, & Agrawal, 2016).

Phishing attacks are often carried out through emails and websites, which are commonly used as communication channels but can also be exploited for deceptive purposes. Cybercriminals use social engineering tactics to deceive people into revealing their sensitive information, such as by replying to fake emails or clicking on links within them. Phishing attacks have become a significant threat to organizations of all sizes and across all industries, with cybercriminals constantly developing new tactics and methods to trick users into revealing their personal information. According to a study by messaging security provider SlashNext, which analyzed billions of link-based URLs, attachments, and natural language messages in email, mobile, and browser channels over a six-month period, found more than 255 million attacks, representing a 61% increase in the rate of phishing attacks compared with 2021 (Oreilly, 2023). Some of the recent phishing scams in history include the 2019 attack on Maastricht University, where hackers used a phishing email to gain access to the university's systems, causing widespread disruption and forcing the university to pay a ransom to the attackers (Bannister, 2020). The 2016 hack of the Democratic National Committee is another notable phishing scam, in which Russian hackers used a phishing email to gain access to the organization's email server, resulting in the release of thousands of confidential emails (Nakashima & Harris, 2018). In 2014, JPMorgan Chase suffered a data breach in which hackers used a spear-phishing email to gain access to employee email accounts, stealing personal information from millions of customers (Roman & Ross, 2014). These attacks not only result in financial losses but also pose a significant threat to individuals' privacy, and their sophistication is making it increasingly difficult to detect them.

From the organizational perspective, the security team employs different metrics to gauge users' awareness and response to potential threats. Among these metrics, reporting rates in phishing simulation exercises are considered an important metric to assess how the organization will respond in the event of a phishing attempt. However, it is crucial to recognize that reporting entails additional responsibilities and costs for users. In this context, it also becomes important for the organization to reassess the threshold at which the costs of encouraging reporting might outweigh the benefits. It is vital to consider the potential loss of labor productivity and opportunity cost to users when imposing this additional responsibility. Striking a balance is essential to ensure that the expectations for increased reporting are realistic and aligned with the users' capacity. Users may prioritize personal safety and perceive ignoring suspicious emails as a suitable course of action, creating a discrepancy between their actions and organizational expectations. This discrepancy poses a challenge in accurately assessing the true scale of the problem and implementing effective countermeasures. Furthermore, reporting rates can be impacted by a variety of factors such as a lack of knowledge and skills related to identifying phishing emails, inadequate infrastructure & support systems that fail to promote necessary incentives, ease, and perceived value in reporting, as well as other factors like fear of reprisal or uncertainty about the reporting process. While previous research supports some of these factors that influence reporting behavior, the understanding of the underlying influences that affect reporting behavior remains limited (Kwak, Lee, Damiano, & Vishwanath, 2020). Therefore, the main objective of this research is to investigate the factors that influence an individual's decision to report or not report phishing emails, with a focus on understanding how to enhance organizational security. By gaining an understanding of these factors, organizations can develop effective strategies to cultivate a reporting culture [1] is an essential aspect of cybersecurity. and improve overall security. This involves enhancing infrastructure and support systems to facilitate a reporting culture and empower individuals in recognizing and responding to phishing attempts. The research will also explore patterns of phishing emails that bypass technical solutions, aiming to educate users on emails that pose a greater risk to their security. By taking a comprehensive approach that considers both organizational and user perspectives, this study aims to contribute to reducing the risk and impact of phishing attacks and ensuring the safety of the organization. This necessitates acknowledging the additional responsibility and cost associated with reporting for users and developing robust infrastructure and support systems that encourage reporting while alleviating the challenges faced by users

3.2 Problem Definition:

In this section, the research problem will be explored. By considering a series of previous studies and the knowledge gaps that appear when analysing previous work that show relevance for further research. Together, this will result in the final problem statement and a description of the scope of the project.

3.2.1 Prior Research:

Prior research has extensively explored the multifaceted nature of phishing attacks and the challenges they pose to individuals and organizations. Phishing attacks, characterized by the deceptive attempt to acquire sensitive information, present a significant threat in today's digital landscape. The consequences of these attacks encompass various aspects such as fraud, theft, harm to reputation, regulatory breaches, and intellectual property

[1] A reporting culture is an organizational environment that encourages individuals to report security threats and incidents without fear of retribution. It fosters open communication, individual initiative (self-efficacy), and clear expectations within the work environment (subjective norms) (Marin, Burda, Zannone, & Allodi, 2023)

loss (Hong, 2012). Phishing is a socio-technical issue that requires addressing both the human and technical aspects (Distler, 2023). Researchers have focused on understanding the measures and processes implemented within organizations to prevent phishing attacks. Studies have highlighted the importance of technical solutions such as email filters, spam detection, and anti-phishing software, as well as organizational policies, training programs, and awareness campaigns (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2008; Stembert, Padmos, Bargh, Choenni, & Jansen, 2015).

Multiple studies have been conducted to investigate the susceptibility of users to phishing attacks, exploring various factors that contribute to this vulnerability. These factors include demographics such as age and gender, as well as individual characteristics like personality type and job role (Vishwanath, Harrison, & Ng, 2018; Lain, Kostiainen, & Čapkun, 2022). Prior research has highlighted persuasive techniques used by attackers in phishing attempts, including social engineering tactics, urgent requests, and mimicry of trusted entities (Jagatic, Johnson, Jakobsson, & Menczer, 2007; Ferreira & Teles, 2019). The authors believe understanding these persuasive principles and behavioral traits can enhance existing detection tools and improve overall security.

Factors influencing an individual's decision to report or not report phishing emails have been explored in prior research. Previous studies have recognized several factors that contribute to the decision of individuals to report or not report phishing emails. These include limited knowledge, ease of reporting, lack of incentives, and concerns regarding potential consequences such as fear of reprisal or uncertainty about the reporting process (Kwak et al., 2020; Distler, 2023). While these factors have been mentioned in prior research, a comprehensive understanding of the underlying influences that impact reporting behavior remains limited.

3.2.2 Research Gaps:

The existing research on phishing prevention has predominantly focused on understanding the responsibility for prevention from either the organizational or human perspective. However, there is a research gap in comprehensively addressing the question of responsibility and collaboration in phishing prevention efforts. It still remains unclear whose ultimate responsibility it is to prevent phishing attacks and how collaboration between the organization and employees can effectively enhance prevention strategies. When exploring the human side, limited research has been conducted on understanding the factors that influence employees' decisions to report or not report phishing emails. This knowledge gap is crucial as it can inform the development of effective phishing prevention and mitigation strategies. By identifying the barriers that hinder employees from reporting phishing emails, organizations can address these issues and promote a reporting culture. Furthermore, gaining insights into the psychological mechanisms underlying reporting decisions can guide the design of targeted training and awareness programs, enhancing individuals' ability to recognize and report phishing attempts effectively.

In addition, there is a notable research gap regarding the specific steps organizations can take to enhance their infrastructure and support systems to foster a reporting culture and combat phishing attacks. While existing literature often emphasizes user behavior and individual responsibility, it tends to overlook the critical role played by infrastructure and support systems in enabling and empowering individuals. Understanding how organizations can strengthen their infrastructure and support systems will contribute to creating an environment that promotes timely reporting of phishing attempts and enhances overall organizational security.

Lastly, another noteworthy research gap lies in the limited exploration of integrating both the perspectives of the security team and the users into a unified approach. Existing literature tends to focus on either the viewpoint of the security team or the users separately, overlooking the potential synergies that can be achieved through their collaboration. Integrating these perspectives in a single research study can provide valuable insights into the dynamics, interactions, and shared responsibilities between the security team and the users in combating phishing attacks.

Overall, addressing these research gaps contributes to the advancement of knowledge and understanding in the field of phishing prevention. By examining the factors influencing reporting behavior, enhancing infrastructure and support systems, and integrating the perspectives of the security team and the users, this research aims to foster a reporting culture, develop effective prevention strategies, and ultimately safeguard organizations' sensitive information against phishing attacks.

3.3 Research Objective

In this case study, set within an educational institute, the primary goal is to explore how the organization can foster a reporting culture to effectively combat phishing attacks. The study delves into understanding the factors influencing reporting behavior and examines the role of infrastructure and support systems in enhancing reporting rates. By analyzing the interplay between user behavior and organizational support, this case study aims to provide valuable insights for designing strategies that promote reporting and strengthen overall security against phishing attacks.

3.3.1 Sub-Research Objectives

- Examine the current anti-phishing measures and processes in place within the organization to prevent phishing attacks
- Investigate trends and patterns in phishing simulation logs to assess the effectiveness of anti-phishing measures in enhancing reporting behavior and identify groups that are more susceptible to phishing attacks
- Analyze phishing emails that bypass technical filters to identify common characteristics and techniques, and assess the effectiveness of phishing simulation emails in replicating them to enhance users' recognition and reporting of such emails.
- Identify the primary factors that influence an individual's decision to report or not report phishing emails.

- Evaluate the current infrastructure support for individuals in recognizing and reporting phishing attempts and propose strategies for improving the infrastructure to enhance reporting rates.

3.4 Research Question

To achieve the research objectives mentioned, the following research question and sub-questions have been formulated.

Main Research Question: How can the organization foster a reporting culture to combat phishing attacks?

3.4.1 Sub-Research Questions

- What measures and processes are currently in place within the organization to prevent phishing attacks?
- What is the current state of clicking and reporting behavior among individuals who have received phishing simulation emails?
- How does the design of phishing simulation emails compare to the characteristics and techniques of emails that bypass technical filters?
- What are the main factors that influence an individual's decision to report or not report phishing emails?
- How can infrastructure and support be enhanced to improve an individual's ability to recognize and report phishing attempts?

3.5 Research Scope:

Based on the research objectives and questions, this study investigates the factors influencing reporting behavior and explores strategies to enhance infrastructure and support systems for fostering a reporting culture in an educational institute in the Netherlands. The research adopts a mixed methods approach, involving qualitative analysis through semi-structured interviews with the security team, faculty, support staff, and students, and quantitative analysis of phishing simulation logs to examine clicking and reporting behavior. By gathering insights from multiple perspectives, the study aims to gain a comprehensive understanding of the problem. The research scope focuses on the specific context of the educational institute in the Netherlands, aiming to identify the key factors impacting reporting behavior and propose recommendations for improving infrastructure and support systems to promote a culture of reporting. The findings of this study will contribute to the field of phishing prevention and provide practical insights for enhancing security practices in educational institutions.

3.6 Thesis Outline:

The thesis is structured into ten chapters, each serving a specific purpose in providing a comprehensive analysis of the research topic. The first chapter presents an executive summary, offering a concise overview of the thesis by summarizing the main research findings and recommendations. Chapter 3 serves as the research introduction, setting the context for the study. It provides background information, defines the research scope, and states the research question and aims. This chapter establishes the foundation for the research and highlights its significance in the field of study. Chapter 4 introduces the case and outlines the research methodology, which follows a mixed methods approach. It further delves into the research methods employed for each sub-research question, including qualitative semi-structured interviews, quantitative phishing log analysis, and document analysis. Chapter 5 conducts a thorough literature review, examining relevant studies and theories related to the research topic. This chapter synthesizes previous research and establishes a theoretical framework that informs the subsequent chapters. Chapter 6 presents the findings from interviews conducted with the IT team and security solution providers. It sheds light on the current processes and measures in place to protect the organization, focusing on the infrastructure perspective from the practitioners' side. Chapter 7 analyzes the phishing simulation log to investigate the clicking and reporting behavior of users. The chapter presents the findings and identifies patterns or trends in the data. Chapter 8 explores the characteristics of reported emails by comparing them to the design of phishing simulation emails. It examines the similarities and differences to identify areas for improvement. Chapter 9 presents the findings from user interviews, which provide insights into the factors that impact reporting behavior. The chapter also discusses ways to recommendations to enhance infrastructure and support systems to foster a stronger reporting culture. Chapter 10 engages in a discussion of the research findings in relation to the existing literature. It explores the implications of the findings, compares them with previous studies, and delves deeper into the topic. The chapter also addresses the validity, reliability, and limitations of the study, while suggesting directions for future research. Finally, Chapter 11 offers a conclusion and practical recommendations based on the research findings. It summarizes the main insights of the thesis and provides actionable recommendations for enhancing the organization's phishing prevention and reporting efforts.

4 Methodology

4.1 Research Approach:

The case study approach is a valuable research methodology that will be adopted in this study to examine the phenomenon of phishing and reporting behavior within an organizational context. A case study is a suitable research approach for this project as it allows for an in-depth exploration of a contemporary event within its real-life context (Yin, 2012). By adopting a case study methodology, the research aims to provide a detailed analysis of the phishing incidents, the organizational culture surrounding security, and the experiences and behaviors of the individuals involved. This approach enables the research to delve into the complex dynamics and nuances of the phishing phenomenon, bringing it closer to the lived reality of employees and the organization (Hodkinson & Hodkinson, 2001).

One of the primary advantages of the case study approach is its ability to generate an in-depth understanding of the bounded system under investigation (Creswell & Poth, 2016). In the context of this research, the case study will allow for a detailed exploration of the organizational practices, policies, and procedures related to phishing incidents, as well as the perceptions, experiences, and behaviors of the different user groups. This depth of analysis will provide valuable insights into the factors that influence reporting behavior and help develop a supportive culture for reporting phishing incidents by enhancing infrastructure and support systems. However, it is important to acknowledge the limitations of the case study approach, particularly in terms of validity and generalization (Yin, 2013). Since case studies typically involve a limited number of cases, generalizing the findings to a broader population may be challenging. In this research, the focus will be on a specific organizational context, which may limit the generalizability of the findings to other organizations. Therefore, the results should be interpreted within the context of the case study organization, and caution should be exercised when applying them to other settings.

4.1.1 Case Study Selection:

The selection of a case study for this research is motivated by the growing threat of phishing attacks targeting educational institutions and the need to understand reporting behavior within this context. Educational institutes, including universities, are increasingly targeted due to the wealth of information available online, such as research, contacts, and sensitive data, which poses a higher risk for potential breaches. According to a study conducted by a security company, Zscaler, the education industry experienced a 576% increase in phishing attempts in 2022, which propelled it from the eighth most-targeted sector to the most targeted sector (Zscaler, 2023).

Universities and educational organizations offer a wide range of digital resources and services to their students and staff members. Moreover, the decentralized nature of universities, with diverse user groups and varying technical capabilities, adds complexity to the security landscape. With the increasing adoption of Bring Your Own Device (BYOD) policies in educational settings, personal devices connected to the university network may lack robust security measures, further amplifying the risk of successful phishing attacks (Bann, Singh, & Samsudin, 2015). By focusing on an educational organization with over 30,000 students, researchers, and personnel, this case study offers a unique opportunity to explore the intricate dynamics of phishing incidents and reporting behavior within a real-life setting. Through an in-depth analysis, this research aims to shed light on the current practices and measures, challenges, and factors that influence reporting behavior, ultimately informing the development of targeted strategies to mitigate phishing threats in educational environments.

4.2 Research Design

4.2.1 Mixed Methods Research

In this study, an embedded mixed methods research approach was utilized to gain a comprehensive understanding of how the organization can foster a reporting culture. The study specifically focuses on two key aspects: the factors that influence reporting behavior and the potential enhancements that can be made to infrastructure and support systems. The embedded design integrates qualitative and quantitative data within a dominant method to provide a more nuanced and holistic understanding of the research problem (Johnson, Onwuegbuzie, & Turner, 2007). The initial phase involves conducting qualitative interviews with the security team to gain insights into the existing measures and processes in place for preventing and addressing phishing attacks. These interviews provide valuable information about the technical measures, educational initiatives, and reporting procedure. Concurrent with the security team interviews, the analysis of phishing simulation logs is performed to examine the reporting rates and identify any patterns or trends. The insights obtained from both the security team interviews and the analysis of phishing simulation logs inform the subsequent phase of the study, interviews with different user groups. These interviews aim to explore participants' understanding of phishing, concerns regarding phishing attacks, confidence in identifying phishing emails, and their experiences with reporting or not reporting suspicious emails. By considering the insights from the security team interviews and the analysis of phishing simulation logs, the interviews with users are designed to delve deeper into the factors influencing their reporting behavior.

By integrating qualitative and quantitative data within the embedded mixed methods design, this study aims to capture a comprehensive picture of the factors influencing phishing reporting behavior. The embedded design allows for the alignment of qualitative and quantitative components, leveraging the strengths of each method. This approach enhances the validity and depth of understanding, enabling a robust analysis of the research problem. While employing an embedded mixed methods approach presents certain challenges, such as data integration and analysis complexities, these challenges are effectively managed through careful design and alignment of the qualitative and quantitative components. By combining these methods, this study aims to provide valuable insights into phishing reporting behavior and contribute to the development of effective strategies for enhancing infrastructure and support to combat phishing attacks.

4.3 Methods in sub-questions

To ensure a thorough and comprehensive analysis, this study will employ a combination of research methods. This section aims to provide an overview of these methods, their objectives, and their relevance to addressing the sub-questions. Three primary research methods will be utilized, as depicted in Figure 1.

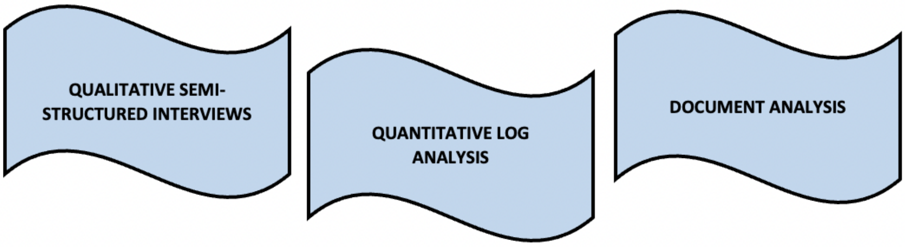

QUALITATIVE SEMI-STRUCTURED INTERVIEWS
QUANTITATIVE LOG ANALYSIS
DOCUMENT ANALYSIS

Figure 1: Research Methods

4.3.1 Qualitative Interviews

Qualitative interviews play a crucial role in gaining in-depth insights and understanding within the research context (Flick, von Kardorff, & Steinke, 2004). In this study, two rounds of semi-structured interviews will be conducted, one with the security team and the other with users, to capture diverse perspectives and experiences. The use of open-ended questions will allow participants to provide detailed and nuanced responses, while closed-ended questions will serve as prompts to explore specific aspects further (Adams, 2015). Semi-structured interviews provide flexibility while maintaining consistency across participants (Dearnley, 2005). They enable the researcher to ask the same core questions to all participants while also allowing for adaptation based on individual responses and roles. This flexibility is particularly valuable when exploring participants' viewpoints, such as understanding organizational protocols and guidelines from different perspectives. By allowing participants to express their independent thoughts within a group setting, a rich and comprehensive understanding of decision-making processes can be obtained (Adams, 2015).

However, it is important to acknowledge that conducting semi-structured interviews can be time-consuming and labor-intensive, requiring interviewer expertise (Adams, 2015). In this study, to address this challenge, a balance was struck by conducting a sufficient number of interviews. A total of 10 interviews were conducted with IT practitioners, taking into consideration their limited time availability due to their professional responsibilities. This sample size was deemed appropriate to gain valuable insights from a diverse range of IT professionals involved in preventing phishing attacks within the organization. Additionally, to capture a comprehensive range of perspectives from the different user groups, a total of 26 interviews were conducted with users, ensuring diverse representation and data saturation (Guest, Bunce, & Johnson, 2006). The larger number of user interviews was motivated by the aim to achieve data saturation, where no new themes or insights emerge from subsequent interviews, thus ensuring a thorough understanding of users' experiences, perceptions, and challenges concerning phishing attacks.

Research Question 1: "What measures and processes are currently in place within the organization to prevent phishing attacks?"

This sub-question aims to investigate the measures and processes currently implemented by the organization to prevent phishing attacks and mitigate potential damage in the event of a successful breach. The research method involves conducting semi-structured interviews with professionals from various teams within the organization, including the Safety, Privacy, and Architecture teams. By conducting these interviews, a comprehensive understanding of the strategies and practices employed by different teams to combat phishing attacks can be obtained while also getting a view of potential challenges they face to safeguard the organization. For this research, a purposive sampling technique will be used to select a total of 10 IT practitioners as participants for the interviews. The sample will be chosen based on their diverse roles and responsibilities within the organization, ensuring representation from teams involved in technical measures, educational initiatives, compliance with regulations, and communication. This diverse sample will provide a holistic view of the organization's approach to phishing prevention and response. Through the semi-structured interviews, participants will be encouraged to share their experiences, challenges, and best practices related to phishing prevention and incident response. The interviews will delve into topics such as technical measures, educational initiatives, compliance frameworks, incident management protocols, and communication strategies. To establish a consistent and reliable point of contact with the organization throughout the research period, one employee will be identified as the main liaison. This employee will assist in coordinating the interviews and facilitating communication between the researcher and the organization.

Research Question 4: "What are the main factors that influence an individual's decision to report or not report phishing emails?"

To investigate the main factors influencing an individual's decision to report or not report phishing emails, a qualitative research method was employed. Both surveys and user interviews were considered as potential research approaches for gathering insights from participants. While surveys offer the advantage of collecting data from a larger sample size, user interviews were chosen as the preferred research method for this study. User interviews provide a more personalized and in-depth exploration of participants' perspectives, allowing for a comprehensive understanding of their experiences, motivations, and challenges. This qualitative approach enables probing questions and the flexibility to seek clarifications, leading to more nuanced and detailed responses. Additionally, user interviews facilitate the exploration of emerging themes and unexpected insights that may not be captured by standardized survey questions. The decision to focus on users was driven by the analysis of quantitative phishing logs and insights from the security team interviews, which indicated a low reporting rate. By engaging directly with users, this research aimed to gain deeper insights into their perspectives, behaviors, and motivations related to reporting phishing emails. The interviews were designed based on the COMB (Capability, Opportunity, Motivation, and Behavior) model, which provides a theoretical framework for understanding and analyzing behavior change (Michie, van Stralen, & West, 2011). The interview questions were tailored to explore users' awareness, knowledge, capabilities, and perceived barriers in reporting phishing emails. Additionally, factors such as the perceived severity of the threat, trust in reporting mechanisms, organizational support, and personal motivation were also addressed to provide a comprehensive understanding of the decision-making process.

Research Question 5: How can infrastructure and support be enhanced to improve an individual's ability to recognize and report phishing attempts?"

Similarly, this qualitative research approach also provides insights into how infrastructure and support can be enhanced to foster a reporting culture. By conducting interviews with users, valuable suggestions and feedback are gathered on how infrastructure support can be improved to enhance their ability to recognize and report phishing attempts effectively. The user interviews serve as a platform for users to share their experiences, challenges, and recommendations, which can be invaluable in identifying areas of improvement in support systems. By analyzing their responses, one can gain a deeper understanding of the specific requirements and needs of users when it comes to infrastructure support.

To investigate the factors influencing individuals' decision to report or not report phishing emails and enhancement of infrastructure support, a mixed sampling approach is being utilized. The sampling procedure involves stratifying the participants based on their user groups (professors, support staff, and students) and their reporting behavior (reported or not reported the previous phishing simulation email). For users who have reported the phishing email from the previous phishing simulation campaign, emails are sent out to invite them to participate in the study. The recruitment process ensures representation from each user group, allowing for a comprehensive understanding of their experiences and perspectives. Insights from these interviews can help understand the perception of the reporting process. In the case of users who have not reported the email, different sampling strategies are employed based on their user groups. For students, a random sampling technique is being implemented outside the library, where every 15th person passing by is approached for potential participation in the study. This approach aims to capture a diverse range of student perspectives across different faculties. On the other hand, for professors and support staff, a convenience sampling approach is being adopted. This involves recruiting participants based on their availability and accessibility. Word-of-mouth and existing networks are being utilized to identify and approach potential participants within these user groups.

4.3.2 Quantitative Phishing Simulation Logs

Research Question 2: "What is the current state of clicking and reporting behavior among individuals who have received phishing simulation emails?"

To investigate the clicking and reporting behavior of individuals who receive phishing simulation emails, a focused research method is implemented. The analysis centers on utilizing the data from the logs of the most recent phishing simulation round. These logs provide valuable insights into clicking and reporting patterns, facilitating the identification of user groups that are more susceptible to falling for phishing attempts and those that exhibit lower reporting rates. Additionally, the logs shed light on the groups that infrequently report phishing emails. By examining the reporting behavior across different user groups, any variations or discrepancies in reporting rates can be identified, contributing to an understanding of the challenges specific groups face in recognizing and reporting phishing attempts. This knowledge can inform targeted awareness and training initiatives. The analysis of the logs places emphasis on various aspects of clicking behavior, including the timing of clicks, such as how quickly individuals click on phishing emails, as well as the time of day when most clicks occur. These insights provide a comprehensive overview of the current state of clicking and reporting behavior, aiding in the development of strategies to enhance cybersecurity awareness and response.

4.3.3 Document Analysis

Document analysis is a research method that involves the systematic examination and interpretation of various types of written or recorded documents.

Research Question 3: "How does the design of phishing simulation emails compare to the characteristics and techniques of emails that bypass technical filters? "

To address the research question on the effectiveness of phishing simulation emails in improving users' recognition and reporting of sophisticated phishing emails, the study employs document analysis. The analysis focuses on a dataset of reported phishing emails collected from 1st March to 15th May. The analysis is two-fold. Firstly, the analysis focuses on the examination of phishing emails that successfully bypassed technical filters. By studying the persuasion principles and techniques employed in these emails, the study aims to understand the specific strategies used by attackers to evade detection. This analysis involves comparing the characteristics of these bypassed emails with the persuasion techniques incorporated in the phishing simulation emails. The goal is to assess the effectiveness of the simulations in raising awareness and improving users' ability to recognize and respond to sophisticated phishing attempts, particularly those that pose higher risks to the organization. Secondly, the analysis extends beyond the persuasion principles to identify broader trends related to target organizations, timing, and frequency of phishing attacks. By examining these trends, the study aims to uncover patterns such as the most frequently targeted organizations and the specific day and time periods when phishing attacks are more prevalent. These insights can inform the development of tailored training materials, enhance user awareness during high-risk periods, and enable the organization to strengthen its network security measures accordingly.

4.4 Ethical Considerations

The research conducted in this study strictly adhered to ethical considerations throughout the entire process. Prior to collecting data, approval was obtained from the Human Research Ethics Committee (HREC) at TU Delft, ensuring that necessary measures were in place to mitigate any potential risks. A comprehensive data management plan was implemented to maintain confidentiality and anonymity of the participants. Measures such as using pseudonyms and other techniques were employed to protect their identities. Participants were fully informed about the study and their rights as research participants, and ethical guidelines were followed to respect their well-being. Informed consent was obtained from all participants before conducting interviews, providing them with information about the study's purpose, their involvement, and any potential risks or harms. Participants had the freedom to withdraw from the study at any point without consequences. The interviews were recorded using Microsoft Teams solely for transcription purposes, and participants were assured of the privacy and secure storage of the recordings, with deletion upon completion of the thesis. Data confidentiality was maintained by treating all participant information as highly confidential and securely storing it according to the Data Management Plan. Personal information was carefully removed before analysis to protect participant identities. These rigorous ethical measures were implemented to uphold the study's integrity and ensure the well-being and privacy of the participants.

5 Literature Review

5.1 History and Evolution of Phishing Attacks

The history of phishing attacks can be traced back to the early days of the internet, with the first known attack taking place in the mid-1990s. At that time, hackers began using randomized credit card numbers generated by algorithms to steal users' passwords from America Online (AOL) (Whitman & Mattord, 2022). These early attacks were conducted via instant messages or emails that posed as messages from AOL employees, which convinced users to reveal their passwords. As attackers learned that requesting customers to update their account information was an effective way to steal sensitive information, phishers began to target larger financial institutions. The term "phishing" was coined in 1996 to describe these attacks, which were also referred to as carding or brand spoofing (Cui, Jourdan, Bochmann, Couturier, & Onut, 2017).

Phishing started to evolve rapidly during the 2000s and 2010s, when people had little knowledge of the practice. Scammers began targeting online payment gateways, such as Paypal and E-gold, stealing user information through fake emails that looked legitimate. In late 2008, the emergence of cryptocurrencies provided an untraceable payment method for hackers, who could then collaborate, extort victims, and securely cash out on their scams (Bartoletti, Lande, Loddo, Pompianu, & Serusi, 2021). Ransomware attacks, which are mainly delivered through phishing emails, also began to increase in frequency and severity, with losses often totaling millions of dollars. In the early 2010s, hackers started to use phishing for purposes beyond financial gain, such as the 2016 politically-motivated phishing attack on Hillary Clinton's campaign chairman, John Podesta.

In present times, phishing attacks are increasing in both sophistication and frequency, with attackers exploiting different channels and threats to trap more victims. Social engineering-based methods are the attackers' weapon of choice, and they continue to focus on such attacks rather than sophisticated techniques and toolkits. The rise of emerging technologies such as mobile and social media has exacerbated the problem, with a large proportion of attacks originating from social media (Marforio, Masti, Soriente, Kostiainen, & Capkun, 2016). According to a report by the Anti-Phishing Working Group (APWG), there were over 1,270,883 unique phishing attacks in the third quarter of 2022, the highest ever recorded (APWG, 2022).

5.2 Types of Attacks and Impact

While the basic premise of phishing remains the same - tricking individuals into giving away sensitive information - the tactics and methods used have become increasingly sophisticated. As a result, there are now many different types of phishing attacks from traditional email phishing to more sophisticated spear-phishing, whaling attacks and BEC (Parmar, 2012). Spear phishing attacks are customized attacks aimed at a particular victim to obtain sensitive information, whereas vishing and smishing attacks are focused on voice and text communications respectively. BEC or Business Email Compromise is a type of phishing attack where the attacker sends an email posing as a high-level executive or manager to a lower-level employee in the finance or accounting department (Bakarich & Baranek, 2019). The aim of the attacker is to deceive the employee into divulging sensitive information or making a financial transaction. On the other hand, smishing is a type of phishing attack that uses text messages as the attack vector, while vishing uses phone calls (Stembert et al., 2015). These attack methods are designed to evade SPAM filters and target more potential victims. Smishing and vishing have become more prevalent due to the widespread use of mobile phones and texting. Criminals use these methods to trick users into revealing personal information or to initiate a financial transaction by pretending to be a legitimate source. These attack methods highlight the adaptability of cybercriminals to leverage new technologies to exploit users. As a result, individuals and organizations need to remain vigilant and aware of these types of attacks to minimize the risk of being victimized.

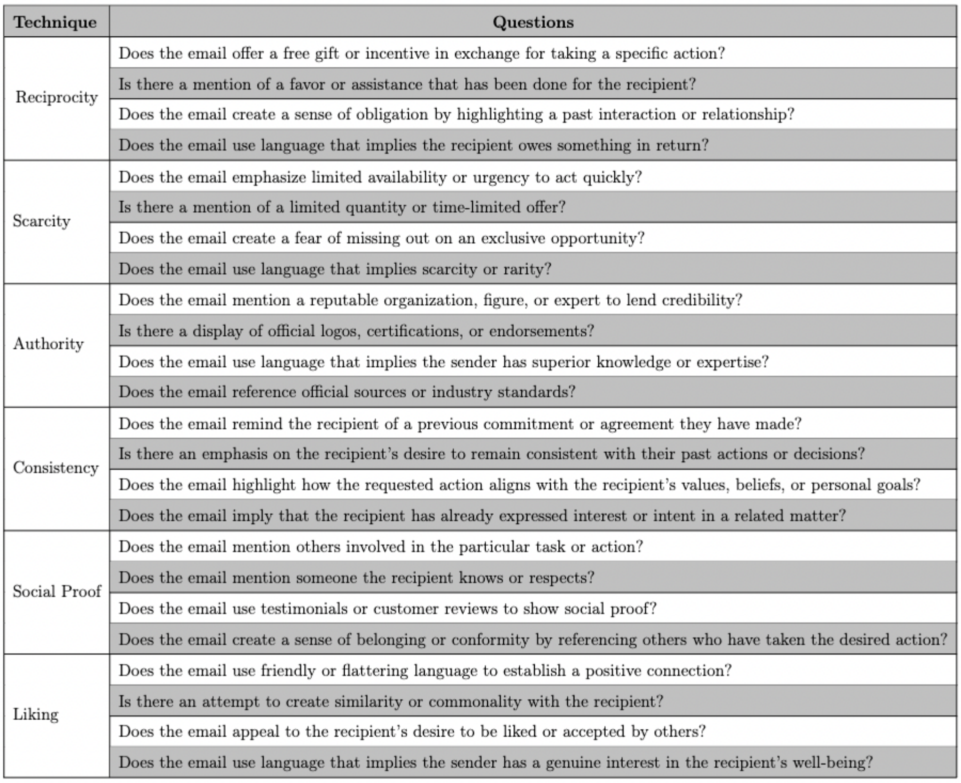
Determining the total damage caused by phishing attacks is challenging due to underreporting and difficulty quantifying the overall impact. A framework proposed by Anderssen in 2012 categorizes cybercrime costs into direct, indirect, and defense costs (Anderson et al., 2012). Direct costs refer to the value of losses or damages suffered by victims, while indirect costs relate to losses or opportunity costs borne by society. Defense costs refer to the value of preventive measures taken to mitigate cybercrime. A study reported that in the United States, phishing attacks cause direct losses ranging from 61 million to 3 billion USD annually (Hong, 2012). However, these figures do not account for significant indirect costs and defense costs incurred. Furthermore, research also highlights that phishing attacks often serve as a starting point for other harmful cyber-attacks, such as ransomware (Masood, Sirshar, & Zainab, 2015). Prior research underscores the significant impact of phishing attacks on individuals, organizations, and society as a whole. These attacks can result in financial losses, damage to reputation, and theft of sensitive information and hence phishing attacks are a serious threat and require continuous attention and effort to prevent and mitigate their impact (Alkhalil, Hewage, Nawaf, & Khan, 2021).

5.3 Persuasion Techniques and Believability of Phishing Emails

With the increasing complexity and sophistication of phishing attacks, it is becoming more difficult for even experienced users to identify and avoid them. This has led researchers to investigate various aspects of phishing emails to understand how attackers are able to convince their targets to take the desired action. Jagatic et al. (2007) stated that phishing emails are successful due to their exploitation of human psychology and interactions. These emails use personal and contextual information to appear trustworthy and persuade victims to give away personal information and money (Jagatic et al., 2007). The authors suggest that identifying various types of persuasive principles and behavioral traits in phishing emails can complement and enhance current detection tools. Similarly, according to a study by Ferreira & Teles (2019), persuasiveness in phishing involves exploiting innate cognitive vulnerabilities in human cognition, such as authority, liking, scarcity, consistency, social proof, and reciprocity—principles of persuasion based on Cialdini's work. These techniques are used to convince the target to perform a desired action. The study found that using persuasion techniques can greatly increase the likelihood of successful victimization(Ferreira & Teles, 2019). Kersten et al. (2022)

conducted a study that identified factors that contribute to the believability of phishing emails across three dimensions: realism, relevance, and persuasiveness (Kersten, Burda, Allodi, & Zannone, 2022). The paper concludes that technical, contextual, language and layout are critical factors in the believability of an email.

Realism is a crucial aspect of phishing emails as it determines the extent to which they resemble legitimate messages. Research has highlighted several key factors that increase a target's suspicion about the legitimacy of an email, including the use of spelling mistakes, bad grammar, unknown links, and inconsistencies in the sender's name and email address (Steves, Greene, & Theofanos, 2020; Parsons et al., 2016). In addition, the visual cues in phishing emails such as logos and conventional formatting can affect their believability (Williams & Polage, 2018). Research also highlights that the context of phishing emails and alignment with the environment of the user can influence how they view the email (Burda, Allodi, & Zannone, 2021). If a phishing email's pretext and other characteristics match the recipient's context, they are more likely to concentrate on the email's convincing aspects and disregard any suspicious cues that could indicate a phishing attack. Understanding persuasion techniques and factors influencing phishing email believability is crucial for developing effective countermeasures and awareness programs (Akbar, 2014). By identifying these factors, individuals can be more vigilant against suspicious cues. A list of questions (Figure 2) has been developed, aligned with Cialdini's principles, to facilitate the analysis of persuasion techniques employed by attackers in phishing emails.



Technique	Questions
Reciprocity	Does the email offer a free gift or incentive in exchange for taking a specific action?
	Is there a mention of a favor or assistance that has been done for the recipient?
	Does the email create a sense of obligation by highlighting a past interaction or relationship?
	Does the email use language that implies the recipient owes something in return?
Scarcity	Does the email emphasize limited availability or urgency to act quickly?
	Is there a mention of a limited quantity or time-limited offer?
	Does the email create a fear of missing out on an exclusive opportunity?
	Does the email use language that implies scarcity or rarity?
Authority	Does the email mention a reputable organization, figure, or expert to lend credibility?
	Is there a display of official logos, certifications, or endorsements?
	Does the email use language that implies the sender has superior knowledge or expertise?
	Does the email reference official sources or industry standards?
Consistency	Does the email remind the recipient of a previous commitment or agreement they have made?
	Is there an emphasis on the recipient's desire to remain consistent with their past actions or decisions?
	Does the email highlight how the requested action aligns with the recipient's values, beliefs, or personal goals?
	Does the email imply that the recipient has already expressed interest or intent in a related matter?
Social Proof	Does the email mention others involved in the particular task or action?
	Does the email mention someone the recipient knows or respects?
	Does the email use testimonials or customer reviews to show social proof?
	Does the email create a sense of belonging or conformity by referencing others who have taken the desired action?
Liking	Does the email use friendly or flattering language to establish a positive connection?
	Is there an attempt to create similarity or commonality with the recipient?
	Does the email appeal to the recipient's desire to be liked or accepted by others?
	Does the email use language that implies the sender has a genuine interest in the recipient's well-being?

Figure 2: Questions to analyze Cialdini persuasion techniques used by attackers in reported emails

5.4 Anti-phishing Measures

Various countermeasures have been applied to prevent phishing attacks. Technical filtering solutions are deployed to prevent phishing emails from reaching their target users. These solutions can use rule-based or machine learning-based techniques to analyze incoming emails and classify them as either legitimate or phishing messages (Fette, Sadeh, & Tomasic, 2007). While machine learning-based techniques have become more effective in detecting phishing websites and can be used to create blacklists (Vrbančič, Fister, & Podgorelec, 2018; Sirigineedi, Soni, & Upadhyay, 2020), attackers can also use similar techniques to bypass these detection systems (Bahnsen, Torroledo, Camacho, & Villegas, 2018). Rendall et al. (2020) emphasize the importance of adopting a multi-layered approach in combating phishing attacks. Such an approach involves implementing various security measures and strategies across different levels of an organization's infrastructure (Rendall, Nisioti, & Mylonas, 2020).

Alternatively, educating users is a proactive method of preventing phishing attacks. By creating awareness about the different types of phishing scams and training users to identify them, this method can help prevent employees from falling victim to phishing attacks and consequently avoid possible information leaks. Additionally, web filtering software or a specific firewall can be used to analyze websites visited by employees and prevent access to sites with malicious intent (Alnajim & Munro, 2009).

5.5 Integrating the Human Factor as a part of the Solution

The field of cybersecurity has historically emphasized the human element as a potential source of vulnerability, leading to efforts focused on excluding, training, controlling, and constraining individuals, often reducing them to mere rule-followers (Zimmermann & Renaud, 2019). However, there is a growing recognition of the need to shift towards a collaborative approach that combines technical measures with human considerations as part of the solution. This mindset shift emphasizes the importance of enhancing factors that contribute to improved recognition and reporting of phishing attempts by users. If the human element is to play a significant role in mitigating risks, it becomes essential to understand how users respond when assigned security-related tasks. If the human element is to play a significant role in mitigating risks, it becomes essential to understand how users respond when assigned security-related tasks. By gaining insights into users' behaviors, motivations, and challenges, organizations can develop strategies that effectively engage users in phishing prevention.

In this context, research by Beautement et al. (2008) provides valuable insights into managing security behavior within organizations. The study investigates the factors that influence compliance with security policies among employees, emphasizing the significance of considering the perceived costs and benefits of compliance from both individual and organizational perspectives (Beautement, Sasse, & Wonham, 2008). By understanding these factors, organizations can design security tasks and policies that align with employees' interests and motivations, fostering a culture of compliance. Similarly, Herley (2009) delves into the rational rejection of security advice by users, highlighting the importance of striking a balance between users' capabilities and the demands placed on them. The study suggests that security advice may present a poor cost-benefit tradeoff, adding to users' burden without providing substantial benefits (Herley, 2009). Recognizing the limitations users face and the potential overload of security tasks, organizations can develop more realistic and effective strategies to engage users in security-related activities, including reporting phishing attempts.

5.6 Phishing Awareness & Training

Different methods are available for cybersecurity awareness training, classified into categories based on their delivery methods - online, game-based, video-based, and simulation-based methods. Each of these methods has its advantages and disadvantages. A review by Chowdhury and Gkioulos suggests that organizations should consider various factors when choosing a method, such as cost, scalability, and level of interactivity (Chowdhury & Gkioulos, 2021). Meanwhile, a study by Abawajy evaluated three delivery methods for cybersecurity awareness, namely text-based, game-based, and video-based methods (Abawajy, 2012). The study found that all methods were successful in increasing the participants' understanding of phishing and its risks, with the video-based method being the most preferred by users. Another study found that gamification of cybersecurity concepts and principles was the preferred mode to raise awareness among students (Beuran, 2016). Tally et al. (2023) recommend incorporating enjoyable and interactive elements into anti-phishing training programs, simulating media and conversations that users willingly participate in during their everyday lives (Tally, Abbott, Bochner, Das, & Nippert-Eng, 2023). Overall, the choice of cybersecurity awareness training method depends on various factors, including the audience, training objectives, and available resources.

5.6.1 Target Groups: Susceptibility to Phishing

Several studies have explored the impact of demographic and personal factors on susceptibility to phishing attacks. Sheng et al. found that individuals between the ages of 18 to 25, and women who have undergone less technical training are more susceptible to phishing attacks (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). Similarly, Jagatic et al. discovered that phishing emails were slightly more likely to be successful when the sender was of the opposite gender to the receiver (Jagatic et al., 2007). On the other hand, Flores et al. found that women are less susceptible to phishing attacks and that computer experience at work and willingness to help correlate with the participant's phishing susceptibility (Rocha Flores, Holm, Svensson, & Ericsson, 2014). Halevi et al. discovered that less suspicious/aware online users are more likely to fall victim to phishing and that conscientiousness can be targeted by attackers to gain a higher phishing response rate (Halevi, Memon, & Nov, 2015). The study by Hong found that gender, trust, and personality are attributes that make some individuals more vulnerable to phishing attacks than others (Hong, 2012). Finally, Butavicius et al. (2012) found that computer-savvy participants were more vulnerable to phishing attacks in the informed experiment, but those with more extroverted or open personalities had better performance in detecting phishing emails in the non-informed experiment (Pattinson, Jerram, Parsons, McCormac, & Butavicius, 2012).

Furthermore, studies have also investigated the impact of people's level of awareness on their susceptibility to phishing attacks. A study by Parsons et al. found that participants who were informed that they were participating in a phishing study demonstrated better performance in identifying phishing emails (Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2015). However, participants with formal training in information systems performed more poorly overall. Educational and awareness activities related to email environments are critical in managing the increased threat of identity theft (Sheng et al., 2010). Signal detection theory has been used to measure vulnerability to phishing attacks, showing that phishing-related decisions are sensitive to individuals' response bias, confidence, detection ability, and perception of consequences (Stanton, Theofanos, Prettyman, & Furman, 2016). Vishwanath et al. (2018) developed the Suspicion Cognition Aromaticity Model (SCAM) model to describe the likelihood of phishing victimization based on individual beliefs concerning cyber-risk, both heuristic and systematic patterns exhibited while processing an email, deficient self-regulation, and developed email habits (Vishwanath et al., 2018). The model uses experiential, dispositional, behavioral, and cognitive factors to provide a more comprehensive explanation of the phishing victimization process. It is evident that various parameters have been identified as affecting susceptibility to phishing attacks, including age, gender, online activity, technical knowledge, education, experience, personality, risk perception, and awareness. Some parameters have shown clear impacts, while others require more research. One approach to training employees could be to use a standardized framework and then develop a customized training regime based on the individual's response to the training and progress using models such as the SCAM.

5.7 Effectiveness of Phishing Training

The effectiveness of anti-phishing training can be improved by various approaches. Firstly, embedded training, which simulate real-world phishing attacks by sending test emails to individuals without prior notification can be more effective than traditional non-embedded training because it simulates real-life scenarios, and users are more likely to learn from their mistakes (Siadati, 2017). According to Kumaraguru et al., users who received embedded training spent more time reading the training materials and showed an improved training effect (Kumaraguru et al., 2008). Additionally, personalized training, which can be based on the user's performance and pace, can increase the effectiveness of training (Carella, Kotsoev, & Truta, 2017). It provides the employees with the impression that the training is customized to their needs, making them more engaged in the learning process. In-class training can have a high short-term impact on the user's ability to detect phishing attacks, but embedded training still outperforms no training or in-class training in the long run (Carella et al., 2017). A study by Karumbaiah et al. observed that users who were exposed to high-quality anti-phishing training videos were less likely to fall for phishing attacks than those who received other types of training (Karumbaiah, Wright, Durcikova, & Jensen, 2016).

The type of phishing attack that users are trained against also affects the effectiveness of training. A study found that embedded training is not as effective against spear-phishing as it is against general phishing (Caputo, Pfleeger, Freeman, & Johnson, 2014). The authors speculated that the training information may not have been perceived as credible, relevant, or interesting by the participants. Lastly, the way in which phishing education is presented to users can significantly impact its effectiveness. Warning messages can be effective in practice, but they must be designed in a way that actively interrupts the user's primary task, requires the user to read the message, and displays clear and understandable choices (Egelman, Cranor, & Hong, 2008). According to Akhawe et al (2013), the experience of the user for a specific warning message has a significant impact on the click-through rate (Akhawe & Felt, 2013). While embedded training in a corporate setting provides a valuable teaching opportunity for users, it is important to recognize that research suggests that immediate feedback and tailored framing alone may not be sufficient to achieve the desired outcomes of reducing click rates or increasing reporting (Caputo et al., 2014). The research conducted by Reinheimer et al. (2020) highlights the importance of incorporating periodic reminders, preferably at least once every six months after the initial training, in phishing awareness programs. These reminders serve as valuable touchpoints for users, reinforcing their knowledge and skills in identifying suspicious emails and staying vigilant against evolving phishing tactics (Reinheimer et al., 2020).

5.7.1 Click Rates

Click rates are commonly used as a metric to assess the effectiveness of phishing simulation exercises. Low click rates are often interpreted as a positive outcome, suggesting that users are successfully recognizing and avoiding phishing emails. However, it is important to note that low click rates do not necessarily indicate training effectiveness and may be influenced by various factors (Steves et al., 2020). Low click rates can result from several reasons. Firstly, if the phishing emails used in the simulation exercises are too easy or lack complexity, users may easily identify them as suspicious and refrain from clicking. Secondly, if the emails are not contextually relevant to most staff, they may perceive them as irrelevant or less threatening, leading to lower click rates. Lastly, if the same phishing scenario is repeated or if the emails are very similar to previous exercises, users who have encountered them before may already be aware of the threat and avoid clicking. Phishing awareness training program click rates should not be solely relied upon as a measure of effectiveness, as they can create a false sense of security, emphasizing the need for a comprehensive metrics-informed approach to combat phishing threats (Greene, Steves, & Theofanos, 2018). In addition to analyzing overall click rates, organizations can also gain valuable insights by focusing on a specific group of employees known as "repeat clickers." These individuals consistently engage in clicking on phishing simulation emails, regardless of the content or context (Lain, Kostiainen, & Čapkun, 2022). By examining the behavior and challenges faced by repeat clickers, organizations can gain a deeper understanding of their susceptibility to phishing attacks and develop targeted strategies to enhance their security awareness and resilience (Fiore, Caulkins, Reinerman-Jones, & Canham, 2019).

5.7.2 Reporting Rates

In addition to the detection of phishing attempts, many training approaches in anti-phishing programs emphasize the importance of reporting suspicious emails to the IT department. Reporting phishing emails plays a crucial role in enabling organizations to respond to ongoing attacks, alert employees, and implement additional countermeasures. However, it is often observed that users tend to report phishing attacks infrequently. Several factors influence the likelihood of reporting a phishing attack. Self-efficacy, which refers to an individual's confidence in performing a specific behavior, plays a significant role in determining whether users will report suspicious emails (Vishwanath, Herath, Chen, Wang, & Rao, 2011). Additionally, the expectation of negative outcomes and an individual's level of cyber security self-monitoring also influence reporting behavior. Customized feedback can also build user trust and encourage the reporting of phishing incidents (Pilavakis, Jenkins, Kokciyan, & Vaniea, 2023). Complicated reporting procedures can also be a barrier to reporting and IT departments need to communicate clearly how and why to report phishing emails (Distler, 2023). Researchers have explored the use of gamification approaches to increase the reporting rates of phishing attacks (Jensen, Wright, Durcikova, & Karumbaiah, 2022a). By introducing game-like elements and incentives, such as badges or achievement milestones, organizations aim to motivate users to actively report suspicious emails. However, there is a delicate balance to be maintained to avoid an excessive number of false positives, where legitimate emails are mistakenly reported as phishing attempts. Striking the right balance involves encouraging employees to report suspicious emails while minimizing the occurrence of false positives, thus preventing an overload of reported emails (Jensen et al., 2022a).

Several studies have used reporting rate as a metric to evaluate the effectiveness of anti-phishing training programs. Studies have reported a significant increase in the reporting rate of simulated phishing attacks after providing regular training to employees (Jensen et al., 2022a; Lain, Kostiainen, & Čapkun, 2022). The reporting rate is a useful metric as it can be directly linked to the ultimate goal of the anti-phishing training, which is to prevent successful phishing attacks. However, it is important to note that reporting rate alone may not be sufficient to determine the effectiveness of anti-phishing training (Lain, Kostiainen, & Čapkun, 2022). This approach has limitations as it does not necessarily reflect the actual behavior of employees in detecting and avoiding phishing attacks. Reporting rate can be influenced by factors such as the ease of reporting, incentives, and company culture, which may not be directly related to the effectiveness of training (Jensen et al., 2022a).

5.8 Theoretical Models:

Understanding the human factor in security is crucial for developing effective strategies to combat cybersecurity threats. Previous studies have employed various theoretical models and frameworks of behavior change to examine the motivations and factors influencing individuals' security behaviors. The Protection Motivation Theory (PMT), the Theory of Planned Behavior (TPB) and Capability-Opportunity-Motivation-Behavior (COM-B) has been used in the context of security, as demonstrated by multiple studies. Yoon et al. (2012) examined college students' information security practices and found that attitudes towards information security were influenced by factors such as perceived severity, response efficacy, response costs, and self-efficacy (Yoon, Hwang, & Kim, 2012). Jansen and Van Schaik (2018) tested the PMT model in the context of fear appeal interventions to reduce the threat of phishing attacks. The study demonstrated the significance of self-efficacy and fear as predictors of protection motivation, and the model's consistency across fear appeal conditions and time (Jansen & Van Schaik, 2018). Menard et al. (2017) integrated self-determination theory (SDT) and PMT to investigate individuals' voluntary secure behaviors in response to threats. The study highlighted the importance of intrinsic motivation and individual-focused appeals in eliciting secure responses (Menard, Bott, & Crossler, 2017).

Shahbaznezhad et al. (2020) utilized the Theory of Planned Behavior (TPB) to investigate the factors influencing users' susceptibility to clicking on phishing emails (Shahbaznezhad, Kolini, & Rashidirad, 2020). Jalali et al. (2020) examined the factors influencing compliance intention and behavior in the context of information security. The study found that TPB factors, collective felt trust, and trust in information security technology were positively related to compliance intention, while workload was associated with the likelihood of employees clicking on a phishing link (Jalali, Bruckes, Westmattelmann, & Schewe, 2020). Van Der Kleij et al. (2021) explored Dutch citizens' cybersecurity behavior using the COM-B model. The study revealed that relevant knowledge, motivation, and opportunity were associated with self-reported cyber secure behavior (Van Der Kleij, Van 't Hoff-De Goede, Van De Weijer, & Leukfeldt, 2021). Van Der Kleij et al. (2020) utilized the COM-B model to explore the interplay between capability, opportunity, and motivation in employee security behaviors to prevent data leakage incidents. The study emphasized the significance of enhancing motivation and opportunity alongside knowledge to influence effective data leakage prevention behavior in organizations (Van Der Kleij, Wijn, & Hof, 2020).

After evaluating the different theoretical models, the Capability-Opportunity-Motivation-Behavior (COM-B) model (Figure 3) was chosen as the most suitable framework for investigating reporting behavior in the context of phishing incidents. The decision to utilize the COM-B model stems from its comprehensive approach, encompassing individual capabilities, environmental opportunities, and motivational factors, which are essential in understanding and influencing reporting behavior.

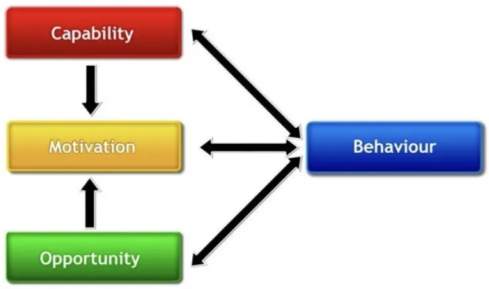


Figure 3: COMB Model of Behavior Change
(Michie, Van Stralen, & West, 2011)

6 Infrastructure & Support

This chapter presents the findings from interviews conducted with stakeholders, including members of the ICT team and security solution providers. The focus is to understand the organization's strategies, practices, and challenges in combating phishing attacks. The chapter delves into the technical and educational measures employed, the procedures and mechanisms for reporting phishing incidents, and the impact and repercussions of such attacks.

6.1 Data collection and interpretation method

In order to gain a comprehensive understanding of the measures and processes implemented by organizations to prevent phishing attacks and mitigate potential damage, a series of semi-structured interviews were conducted. The interviews were conducted with 10 ICT practitioners who represent various teams within the organization's ICT department as well as security solution providers. The team consists of both internal and external consultants. The list of participants can be found in Table 1.

Table 1: Overview of Interviews

Participant Code	Role/Team	Company Code
P1	Engineer	C1
P2	Engineer	C1
P3	Privacy	C1
P4	Privacy	C1
P5	Manager	C1
P6	Security Consultant	C1
P7	Awareness	C1
P8	Awareness	C2
P9	Engineer	C3
P10	Awareness	C3

After a short introduction of the purpose of the study and the interview, all respondents were asked to sign an informed consent form, either written or orally. This explained that data would not be shared, only in an aggregated and anonymized way. All participants gave permission to record the interview on audio. All interviews were held online via MS Teams due to preference by the interviewee. The interviews took on average 33 minutes, with the shortest 25 minutes and the longest 49 minutes. A narrative analysis approach was employed to interpret and analyze the qualitative data collected from the interviews. The focus of the analysis was on capturing the participants' experiences, challenges, and best practices related to phishing prevention and incident response. By carefully reviewing and interpreting the interview transcripts, valuable insights and narratives were identified, providing a deep understanding of the strategies and practices employed to protect the organization.

6.2 Technical Measures

During the research interviews conducted with the ICT team, several key insights were revealed regarding the technical measures employed to combat phishing emails and enhance email system security. The participants highlighted the role of various technologies, such as robust email filters, spam detection algorithms, and malware scanners, in identifying and blocking suspicious emails with potential phishing attempts. The team mentioned the use of multiple solutions to strengthen email security - " *We have multiple solutions that we use. Solution from [C3] is the first line of defense. Then it will be redirected through our Linux systems and then it will be delivered at the Microsoft Exchange, which also has its own checks in place."[P1]* The participants mentioned this multi-layered approach is an important part of the organization's strategy to safeguard against phishing attempts.

Participants highlighted the role of email filters in detecting and preventing phishing emails. These filters utilize various techniques including machine learning algorithms to categorize emails - *"so we also filter based with engines that use machine learning for spam and phishing through which can analyze patterns and behaviors to identify more sophisticated and targeted phishing attempts." [P9].* Additionally, the organization recognizes the differing risk profiles and hence has implemented different filters - *"we're differentiating between students and employees, with both of them on two different systems. Employees are more at risk within the organization because they're using more corporate-sensitive data than students. So that's the reason why we put all employees behind a more sophisticated e-mail filter." [P5]* The participant highlighted this distinction ensures that employees, who handle more corporate-sensitive data, are provided with a more sophisticated email filter to mitigate their higher risk.

In addition to email filters, participants also mentioned how URL rewrites strengthen the organization's defense against phishing attacks. By employing URL rewrites, the organization tries to protect users both message delivery and when interacting with links in emails - *"we do URL rewrites so that you are protected when the message gets delivered, but also when you click on the message." [P6]* This approach ensures that users are protected from potentially malicious websites. The system acts as the 2nd line of defense - *"if somebody clicks on the link, basically the system goes to check the link before you get to see the data, and then if it turns out to be phishing, then we know... it got blocked on the 2nd check."[P7]* These insights highlight the email security approach employed by the organization, which encompasses advanced email filters, user segmentation based on risk profiles, and the implementation of URL rewrites to protect the organization.

6.2.1 Challenges

While the technical measures implemented by the organization offer protection against phishing attempts, they are not without their challenges. One of the challenges encountered is the increasing sophistication of attackers in their attempts to bypass email filters. As Interviewee P5 acknowledged, *"It's a cat and mouse game... they always find new ways to come through the filters. "[P5]* Attackers continuously evolve their techniques to bypass detection, requiring constant updates and adjustments to the email filters to stay ahead. Another challenge lies in the detection of highly targeted and sophisticated phishing attempts - *"When it becomes more targeted, that's when it becomes also more interesting for security analysts to look at it first as well." P[9]* They highlighted that identifying and distinguishing these advanced threats from legitimate emails can be a complex task, requiring thorough analysis and expertise from security analysts.

Another challenge mentioned with the technical measures is the dynamic nature of phishing attacks. They emphasized the clever tactics employed by attackers, explaining, *"Attackers are smart, right? They will just set up the Office 365 account, they will put out some malware on there. The site will be completely legit, and if you are patient zero, we don't know it's the first time that something is coming from that Office 365 account, so it gets delivered. Then 15 minutes later, you change the content behind it, you make it into something phishing or malicious, right? But then the message has already been delivered." [P9]* This highlights the ongoing challenge of identifying and blocking malicious URLs in real-time to prevent users from accessing harmful content. Addressing this challenge requires continuous monitoring, rapid response mechanisms, and the ability to quickly update filters and block pages to keep pace with evolving phishing techniques. Another challenge lies in the occurrence of false positives, where legitimate emails or websites are mistakenly flagged as phishing attempts. *"The other day we had this event in Spain which a few of our employees even attended and they received a newsletter of this event passed through but the URL of this website got blocked because there might have been some suspicious activity which was detected by [C3]. I visited the website myself outside of our environment... and I couldn't see anything, there was nothing weird going on. So this was a false positive." [P2]* False positives can disrupt normal communication and cause inconvenience for users, as they may be wrongly notified and prevented from accessing legitimate resources. Despite the robustness of the technical measures in place, achieving 100% accuracy in filtering out phishing emails remains a challenge. *"Currently, our email filter is able to successfully filter out 99.4% of the emails." [P7]* While this indicates a high success rate, it also means that a small fraction of phishing emails still manage to bypass the filter. All participants emphasized the importance of reporting phishing emails as a crucial step in addressing the challenges posed by sophisticated attacks that can bypass technical measures, as it provides valuable feedback for enhancing email security protocols, enabling proactive improvements, and strengthening the overall defense against phishing attempts.

6.3 Reporting Process

The reporting process for suspicious emails within the organization plays a crucial role in identifying and mitigating potential threats. To report a suspicious email, users are typically required to forward it to a designated abuse-handling email address. However, in certain cases, particularly when further analysis is required to determine the email's nature, the security team requests users to save, extract, and attach the email for header analysis. Once received, the Security Incident Response Team (SIRT) takes charge of handling these reports and initiates an investigation. Upon receipt of a report, they conduct an initial assessment to determine if any previous reports of the same email exist. This step helps prevent duplication of efforts and ensures efficient utilization of resources. "*The reports can come into the mailbox and can be sent via top desk" [P1]* which indicates that multiple channels are available for users to report suspicious emails conveniently.

The content of the reported email is analyzed by the SIRT team. They look for potential indicators of phishing attempts, such as bad grammar, suspicious sender addresses, and links that could lead to malicious websites. "*We decode this link and then I usually open a sandbox. Through the sandbox, I'm going to look on in the website itself...to figure out what this person could have done." [P2]* This investigation helps in understanding the nature and severity of the threat, enabling the team to respond effectively. Upon confirming a reported email as a phishing attempt, appropriate actions are taken - "*when we can see that it is malicious ourselves, then we can block it within minutes. And so then we can just edit it on our systems and have it blocked."[P1]* The SIRT team blocks the sender to prevent further communication and takes measures to prevent outgoing network traffic associated with the email. Additionally, the findings from reported emails contribute to the continuous improvement of the organization's email filters. *"The information of this message will also be used to adjust the email filters to block similar messages in the future."[P5]* This iterative process ensures that the email filters are constantly updated.

6.3.1 Challenges

The reporting process, while essential for identifying and mitigating phishing attempts, also presents several challenges that impact its effectiveness. One notable challenge is the absence of a dedicated reporting button within email clients, which can make it less intuitive for users to report suspicious emails. While implementing such a button is technically feasible within the organization's license, it requires a cumbersome process of deployment across all employee computers. This approach is time-consuming and not compatible with different email clients and operating systems. As Interviewee P6 remarked, *"Not everyone uses Outlook. You have a lot of email clients, so of course, a lot of people use different email clients."*The diverse range of systems and email clients used by employees, including Chromebooks, Linux, Windows, macOS, Android, and iOS, further complicates the implementation of a universal reporting button. Interviewee P1 humorously remarked, "*Sometimes I wish we functioned like a bank. So everybody has one computer and you can only use one application for emails.*" The remark underscores the complexity faced by the organization due to the wide variety of systems and email clients used, making it challenging to establish uniformity in reporting and security practices. Furthermore, the volume of reported emails, especially the phishing simulation campaigns can be overwhelming for the Security Incident Response Team. In order to manage the volume of reported emails and optimize resource allocation, the organization has implemented message templates that need to be manually triggered to acknowledge receipt of the reported emails. *"The implementation of the report button could reduce our workload since we won't have to initiate the automated reply for every email manually. [P2]"*

6.4 Educational Measures

The educational measures implemented by the organization encompass multiple aspects. Firstly, there is a centralized website that serves as a repository of information regarding security and privacy, including resources on how to recognize phishing attempts. The participants highlighted the importance of disseminating information about guidelines and best practices to users and how the Privacy and Security website suits that purpose. *"The website provides basic information so people have a place to go to, to find information, and everything is in one place. That was really important." [P3]* Secondly, the organization conducts training sessions and e-learning activities to enhance individuals' knowledge and awareness. These initiatives aim to equip employees and students with the skills and understanding necessary to identify and respond appropriately to phishing attempts. "*We try to do trainings and also have sessions on safety compliances. We organized escape room challenges to promote good password habits.[P6]*" The organization views these initiatives as a way to empower individuals with practical skills and reinforce the importance of cybersecurity best practices.

The organization recognizes the importance of reaching out to a wider population and conducts awareness programs through various channels. While at a nascent stage, over the last year, the organization has stepped up the effort to reach out to various user groups through collaborative efforts with faculties to conduct awareness campaigns, stating - *"we also collaborate with people in the faculties to conduct awareness campaigns, although this is still in the early stages and hasn't seen many outcomes yet." [P4]* The organization considers the involvement and collaboration with department heads as a part of the strategy to reach out to a wider network and raise awareness on security matters. The organization also organizes an annual security week in October, during which various activities and workshops are conducted to engage and educate users on essential topics like password management and identifying phishing attempts. " *"One significant event we utilize is the security week where we organize activities to raise awareness about password management and phishing attempts, providing valuable tips for identifying phishing emails."[P6]*

Lastly, participants mentioned that the phishing simulations are a crucial component of the university's educational measures, aiming to replicate real-life phishing attempts in a controlled environment. The organization believes these simulations serve as learning experiences, allowing participants to gain firsthand exposure to common phishing tactics and develop the skills needed to identify and respond to fraudulent emails. *"The objective of our phishing simulations is to create a safe environment for users to experience and learn about common phishing tactics." [P7]* During the phishing simulations, participants are provided with feedback and guidance on recognizing phishing attempts and improving their responses. *"So when a person clicks, they are being informed, they have clicked on the phishing link on the link and the phishing e-mail simulation. Um, they get the information on how to recognize it the next time and how they should have been able to recognize it for the specific e-mail, and we also give some information about the report procedure."[P8]* The organization believes this feedback mechanism allows individuals to understand the specific indicators they missed in the simulated phishing email and provides them with actionable knowledge to identify similar threats in the future.

6.4.1 Challenges:

The educational measures implemented by the university face several challenges that affect their effectiveness and reach. One significant challenge arises when assessing user awareness and response, particularly in the context of phishing simulations. While click rates for these simulations are high, indicating user engagement with the simulated phishing attempts, the organization is unsure about users' ability to detect phishing attempts and their awareness of the importance of reporting, as reflected by the relatively low reporting rates. Interviewee P5 highlighted this concern, stating, *"Click rates are high, but reporting rates are low."* It is important to note that while low reporting rates may suggest a lack of user awareness, it is also possible that some users are aware of the phishing attempts but choose to ignore them. However, making assumptions about user behavior without concrete evidence can hinder the organization's efforts to enhance user awareness and response.

Another challenge lies in effectively communicating technical information to a non-technical audience. *"Trying to translate the complexity of information security and privacy to easily understandable instructions for people." [P7]* is a significant challenge. Participants also highlighted privacy and cybersecurity topics might not be as exciting or popular as other subjects, which makes it challenging to keep users engaged and motivated in educational programs and secure practices - *"The topic honestly is not something that many people find sexy. It's not a topic that many people think, 'Oh wow, interesting article about privacy."[P7]* Unlike trendy subjects, discussions about privacy and cybersecurity may not immediately grab attention or generate enthusiasm. As a result, it becomes more difficult to sustain users' interest and commitment to learning and implementing security measures. Lastly, participants emphasized the challenge of reaching out to a large number of users in the organization, with one participant stating, *"for a campus with 40,000 people, achieving widespread reach becomes challenging." [P4]*

6.5 The Security Team's Perspective

6.5.1 Potential Consequences of a Phishing Attack

A successful phishing attack on an organization can result in various consequences, each carrying its own significance. One of the primary concerns is the unauthorized access to sensitive data. *"If someone gains access to an employee's or student's account, unauthorized people can potentially access research data, organization systems, and other storage applications." [P4]* Intellectual property, research data, and confidential information are at risk in such scenarios. Breaches of sensitive data can lead to severe consequences for the organization, including compromised research projects, potential risks to research participants, and violations of data protection regulations. Financial implications are another significant concern arising from successful phishing attacks. Unauthorized access to financial records, customer data, or other sensitive information can result in financial losses for the organization. *"If an attacker successfully gains access to sensitive data, it constitutes a data breach under GDPR. In such cases, if authorities determine that the organization did not implement adequate security measures, we could potentially face financial penalties."[P3]* Lastly, reputational damage is a major concern following a successful phishing attack. *"A data breach can lead to the conclusion that the organization has not done what it should.[P3]"* The participants highlighted that the loss of customer trust, damage to brand reputation, and negative public perception can have long-lasting consequences for the organization's relationships with stakeholders, partners, and the broader community.

6.5.2 Importance of Reporting:

Reporting plays a vital role in the overall cybersecurity strategy of the organization, serving as a crucial mechanism for promptly identifying and addressing potential security threats. When individuals report suspicious activities or phishing attempts, they become active participants in the collective defense of the organization. *"If an email is not reported at all because everyone thinks someone else did, then the organization is at risk." [P4]* Low reporting rates can leave the organization vulnerable, as incidents may go undetected and unaddressed for extended periods. Moreover, reporting incidents helps organizations improve their systems and enhance their security measures. *"I would love to get it higher of course as mentioned because this will also help us see how to improve, where to, how to and where to improve our systems." [P1]* The participants mentioned by analyzing reported incidents, the organization can gain valuable insights into the types of threats targeting their users and identify areas for improvement. Reporting provides essential data for updating technical filters, refining security protocols, and developing targeted training programs to address specific vulnerabilities. It empowers the organization to proactively enhance its defenses and stay ahead of evolving cyber threats.

While the organization strives for higher reporting rates to gain a better understanding of overall awareness among users, the importance of quick reporting cannot be overstated. *"The sooner we get a report from an email, the better we can protect the rest of the campus." [P7]* This urgency becomes even more critical in cases like CEO fraud. Another participant highlighted the significance of response time, stating, *"For us, it is important to know how quickly someone reports an email. Like I said in the case of CEO fraud, the sender puts a lot of pressure and is very active with these emails. The more they talk with each other, the more that trust is built, and the more likely it is that they will send the gift cards or buy something. So response time is important in a lot of cases. It's also very important because we need the information as quickly as possible so we can do our analysis"[P2].* Swift response time plays a critical role in cutting off further communication between scammers and employees, minimizing the risk of fraudulent actions. Additionally, quick reporting enables the organization to promptly analyze and assess the associated risks, allowing for immediate mitigation measures. Participants mentioned the faster the information is received, the more effectively the organization can respond and safeguard itself against cyber threats. In the context of phishing simulations, the organization strives for higher reporting rates as they serve as a valuable metric to gauge the overall awareness within the organization. *"We want to raise awareness on the behavior that you should have when you receive a phishing e-mail. So we are trying to make people aware like, hey, if you receive a phishing e-mail, many people are not aware that they should report it.[P7]"* By encouraging individuals to report simulated phishing emails, the organization can gain insights into the level of understanding and engagement among their users.

6.5.3 Clash of Perspectives: The Security Team's Side

One valuable insight gained from the interviews is the ICT team's understanding that security measures can sometimes be seen as an annoyance by users. Users may not always fully understand the reasons behind the implementation of certain security steps. This lack of understanding can contribute to their dissatisfaction and perception that such measures only make their tasks more challenging. *"When we implement multi-factor authentication, employees often express their dissatisfaction, considering it an extra and inconvenient step. They fail to see how this extra step is actually keeping them safe. We often hear feedback that we're making things more difficult, but our intention is not to inconvenience users; rather, it's to enhance security." [P5]* The security team recognizes that users may not always be fully aware of how their actions can impact the overall security of the organization. Users might not understand the potential consequences of their behavior and how it can either contribute to or mitigate security risks. In the context of phishing - *"many people think I didn't click it. I deleted. That's fine. And yes, in the individual case that's fine because you mitigated the risk, but you could have contributed to the protection of the organization by reporting it. You know you get an e-mail you wouldn't immediately think that you can protect the university by reporting it so you think, I'll delete it and get it out. So it's basically the human behavior or the customs that they're used to."[P7]*

The security team views cybersecurity as a team sport, recognizing that finding a balance between security and usability is crucial. They strive to avoid limiting users' autonomy and freedom within the ICT environment. *"You know, from the ICT team's perspectives, I think you should make some kind of playground and if you're within the playgrounds, you can do whatever you like and as long as you stay within the fences of the playground you can play with whatever tools you can find and do whatever you like... So that's basically the strategy and the balance we're trying to find between the users and ICT technology because if we don't, then they're going to shop somewhere else." [P7]* The security team hopes this collaborative approach will allow them to understand user needs, provide necessary support, and prevent users from resorting to external solutions that may compromise security. Furthermore, the team views transparency and clear communication as important factors when developing infrastructure and support systems. *"I believe that consistency and clear communication are crucial when it comes to cybersecurity awareness and education. It's important for us to practice what we preach and communicate in a way that is consistent and recognizable for everyone in the organization.[P4]"*

6.6 Chapter Summary

The goal of this chapter was to understand the measures and processes implemented by the organization to prevent phishing attacks. The findings reveal that the organization employs a comprehensive approach, incorporating both technical and educational measures. In terms of technical measures, the organization follows a multi-layered approach by partnering with different companies that provide a range of solutions. Regarding educational measures, the organization places a strong emphasis on raising awareness among its users. They employ various initiatives, with a particular focus on conducting phishing simulations, to equip users with the knowledge and skills needed to identify and respond to phishing attempts. However, challenges exist in this area, such as low reporting rates for simulation exercises. To address this, the organization recognizes the importance of fostering a culture of reporting and emphasizes the significance of reporting suspicious activities for the organization's overall security. Additionally, the organization is also searching for solutions to make the reporting process more efficient. Lastly, the organization recognizes that cybersecurity is a team effort and strives to balance security measures with user experience. They understand the importance of user cooperation in effectively preventing phishing attacks. By finding this balance, the organization aims to protect itself without causing unnecessary inconvenience to its users, promoting a collaborative approach to cybersecurity.

7 Phishing Simulation Logs

This chapter delves into the analysis of phishing simulation logs, which provide valuable insights into the design and effectiveness of phishing campaigns. The first section of this chapter presents the process involved in designing the phishing simulation campaign. The second section focuses on the characteristics of phishing emails, including their design elements, frequency of campaigns, and the metrics used to assess their success. Here, insights from the interviews with the security team will also be shared wherever necessary. The subsequent section presents a detailed analysis of the most recent phishing simulation round. This analysis encompasses multiple aspects, including the number of emails sent, click rates, reporting rates, and the time elapsed from email delivery to link clicks (specifically for individuals who clicked the link). Furthermore, the study examines the time of day when users opened the link and assesses user engagement on the landing page to which they were redirected (upon clicking the link), based on the number of clicks. This analysis is conducted across three distinct user groups: students, faculty, and support staff. By examining these key metrics and user behavior patterns, a comprehensive understanding of the effectiveness of the phishing simulation and its impact on different user groups can be gained. These findings will contribute to the development of targeted cybersecurity awareness and training programs to mitigate the risks associated with phishing attacks

7.1 Designing the Campaign

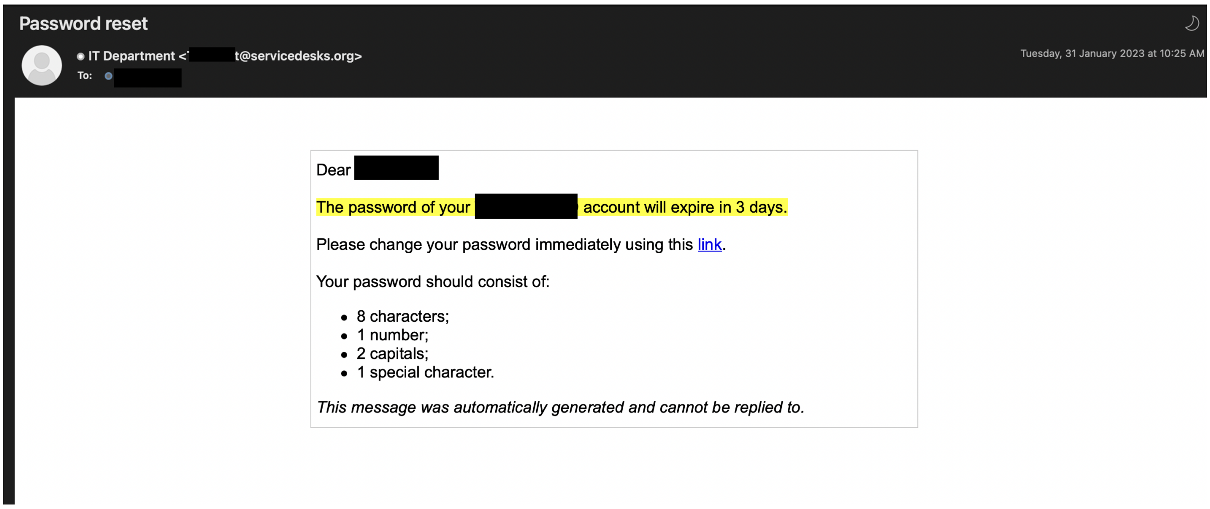
The design and customization of the phishing campaigns are integral to the collaborative efforts between the organization and its partner company, which specializes in raising awareness and implementing tailored campaigns for various organizations. The design of the phishing emails is driven by the goal of closely emulating the techniques used by real cybercriminals. *"So that is the underlying theory that we're using - the use of persuasion principles. So people are more likely to click when you try to convince them in an e-mail, for example, by adding time pressure in the phish e-mail or adding authority in it, for example." [P8]* This approach aligns with the principles of marketing and social psychology, which are widely employed by the partner company when designing these campaigns. By leveraging these principles, the campaign aims to accurately simulate the threats faced in real-world scenarios.

The partner company's approach is to customize the campaigns, tailoring them to match each organization's unique characteristics and specific needs. For instance, considering the organization's periodic request for password resets, the phishing campaigns may leverage this context to create a sense of urgency and familiarity. By incorporating specific attributes and cues relevant to the organization, the partner company ensures that the phishing simulations are contextually aligned and resonate with the recipients. The participant mentioned, *"We have the cue types or the red flags in the phish email, and you have the relevance or the context to the user or to the recipient of the email, and I think those two combined are giving you some type of complexity score." [P8]* By combining cues and relevance, the campaign aims to create a more complex and persuasive email, increasing the susceptibility of users to engage with the content.

The organization utilizes three key metrics to assess the success of the phishing simulation campaign. Firstly, they track the number of individuals who receive the simulated phishing email, as they have access to the recipient list. Secondly, they measure the number of people who click on the link within the email, indicating a potential vulnerability to phishing attacks. Finally, they monitor the number of users who report the email, demonstrating an awareness and active participation in maintaining security. These metrics are assessed at a departmental level rather than on a personal level, allowing the organization to gauge the effectiveness of the campaign across different groups. The organization conducts phishing campaigns four times a year, taking into account the impact on employees. The company avoids scheduling campaigns during critical periods such as exams or summer holidays to prevent unnecessary inconvenience. *"We schedule our phishing simulation on a moment that we think is the best time to bother people basically because you're still bothering them obviously." [P7]* They recognize that repetition is crucial for effective learning, but they also acknowledge the importance of avoiding excessive repetition to maintain employee engagement. By strategically planning the frequency and timing of the campaigns, the organization aims to strike a balance between teaching employees about phishing threats and minimizing any potential disruption or frustration.

7.2 Round 2 Simulation Email

In this section, the second email of the four-round phishing simulation campaign is analyzed. The email was distributed to all users, and specific measures were taken to ensure its successful delivery. Email filters were intentionally turned off to bypass any security measures that could potentially block the email. The timing of the email distribution was limited to the working hours between 8 AM and 6 PM, when users are actively engaged with their email accounts.



Password reset

IT Department <[redacted]t@servicedesks.org>

To: [redacted]

Tuesday, 31 January 2023 at 10:25 AM

Dear [redacted]

The password of your [redacted] account will expire in 3 days.

Please change your password immediately using this link.

Your password should consist of:

- 8 characters;
- 1 number;
- 2 capitals;
- 1 special character.

This message was automatically generated and cannot be replied to.

Figure 4: Round 2 Phishing Simulation Email

The phishing email (Figure 4) used in the simulation aims to deceive users by closely resembling legitimate password reset requests. It employs a minimalistic design, free from images or visual elements that could raise suspicion or trigger email filters. The email uses social engineering techniques to manipulate recipients' emotions and behaviors. It creates a sense of urgency by notifying recipients that their account password will expire in three days. This urgency prompts immediate action without thorough scrutiny of the email's legitimacy. To enhance the email's credibility, specific password requirements are mentioned such as an 8-character password, including 1 number, 2 capital letters, and 1 special character. These detailed requirements aim to convince recipients that the email is a genuine communication from the organization. Lastly, the email adopts an impersonal tone and explicitly states it cannot be replied to, adding an authoritative layer and discouraging recipients from seeking clarification. This tactic exploits individuals' tendency to trust and follow instructions without questioning their authenticity.

7.3 Results of the Phishing Simulation Exercise

This section offers a comprehensive analysis of the 2nd round of the phishing simulation exercise conducted by the organization, including metrics such as email volume, click rates, reporting rates, time from email delivery to link clicks, timing of link clicks, and user engagement on the educational landing page.

7.3.1 Results Overview

As depicted in Figure 5, out of the 42,417 emails sent in the phishing simulation, a total of 11,085 users (26.1%) were lured into clicking on the link in the email. Additionally, 2,610 users (6.1%) reported the email as suspicious. However, it is important to acknowledge that the behavior of the remaining users who did not fall for the phishing attempt is uncertain. It is unknown whether they opened the email or deliberately chose to ignore it.

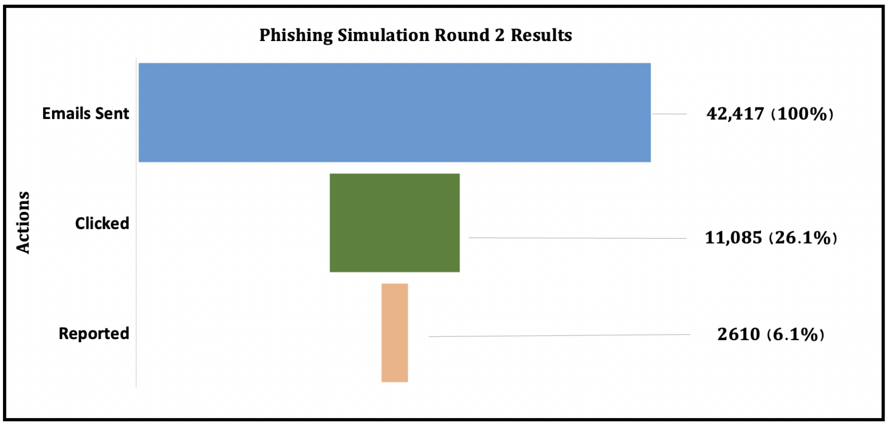


Figure 5: Round 2 Phishing Simulation Results

7.3.2 Click-rates by User Group

The findings from the phishing simulation analysis (Table 2) reveal interesting patterns across different user groups. The user groups in focus include students, faculty, and support staff, each representing distinct roles within the organization. Students encompass individuals enrolled in various Bachelor's and Master's programs, while the faculty category comprises professors and researchers. Support staff comprises individuals serving in diverse functions within the university, excluding students and faculty. The click rates varied across the different user groups. The highest click rate was observed among students, with 27.65% of the total student population falling for the phishing attempt. Faculty members exhibited a similar susceptibility, with a click rate of 26.47%. In contrast, support staff demonstrated a relatively lower click rate of 15.78%. These findings suggest that students and faculty members may be more vulnerable to engaging with phishing emails compared to support staff.

Table 2: Phishing Simulation Round 2 Click Rates

User Group	**Total Population**	**Users Clicked**	**Click Rate (%)**
Faculty	8,928	2,363	26.47%
Student	28,951	8,006	27.65%
Support Staff	4,538	716	15.78%
Total	**42,417**	**11,085**	**26.13%**

7.3.3 Time Interval between Receiving and Clicking

The analysis of time intervals between email receipt and link clicks in the phishing simulation email reveals insights that shed light on user behavior and response patterns (Table 3).

Table 3: Time Interval Between Receiving and Clicking on Link (in Minutes)

Time Interval (Minutes)	**Frequency**	**Percentage**	**Cumulative Percentage**
<1 Min	275	2.48%	2.48%
1 to 5 Mins	451	4.07%	6.55%
5 to 15 Mins	554	5.00%	11.55%
15 to 60 Mins	1265	11.41%	23.96%
60 to 720 Mins	3239	29.22%	53.18%
720 to 1440 Mins	1227	11.07%	64.25%
Beyond 1440 Mins	4074	36.75%	100%
Total	**11085**	**100%**	**100%**

Examining the shorter intervals (Figure 6) reveals a significant trend, with a notable percentage of users clicking on the phishing link within the first few minutes. Specifically, 2.48% of users clicked within the first minute, 4.07% within the first five minutes, and 5.00% within the first 15 minutes. These findings suggest that a considerable percentage of users (11.55%) might be more susceptible to engaging with phishing emails within minutes of receiving the email. Furthermore, the analysis revealed that nearly one-fourth of users who fell for the phishing attempt did so within the first hour (23.96%). This statistic emphasizes the importance of prompt identification, reporting, and appropriate response to phishing emails to protect the organizaiton. Looking beyond the first hour, 53.18% of users clicked on the link within the first 12 hours. The remaining time intervals, classified as the "Rest" category, encompass 36.75% of users. This segment includes users who clicked on the link beyond the initial 24-hour period.

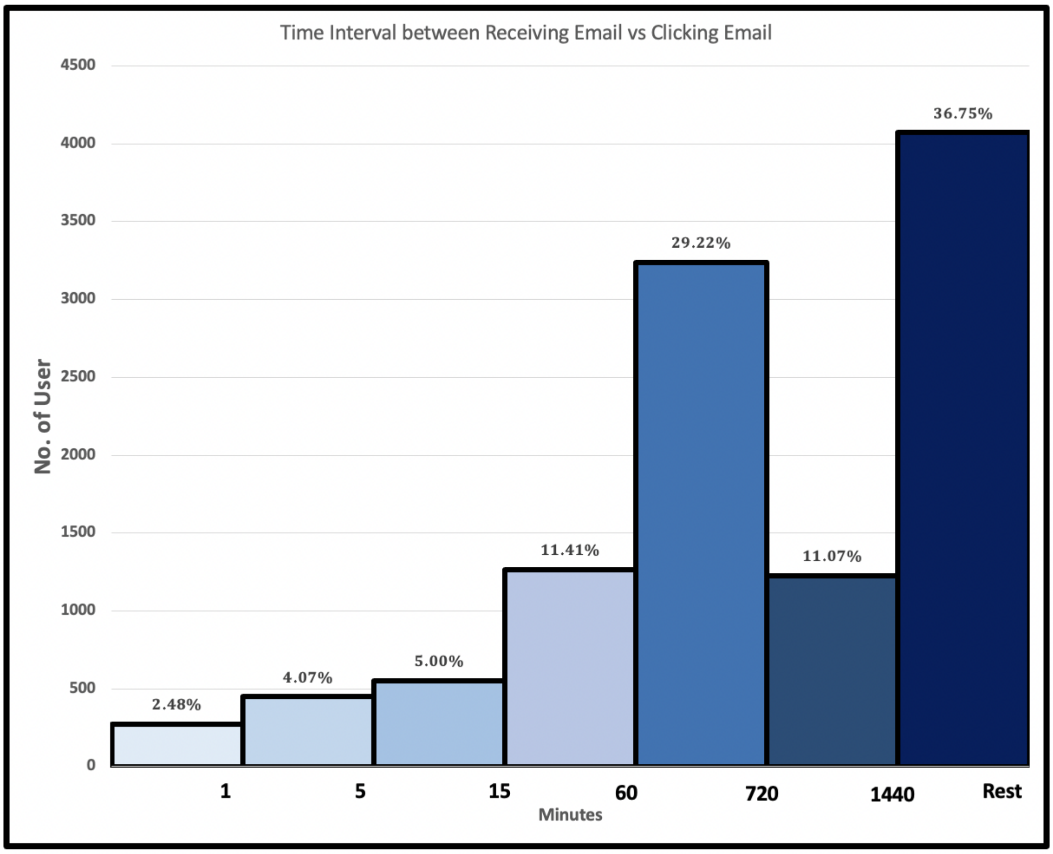


Figure 6: Time Interval Analysis: User Response to Phishing Email

7.3.4 Click Frequency by Time Interval

The analysis of click frequency by time interval (Figure 7) in the phishing simulation campaign provides insights into the temporal patterns of user engagement with the phishing simulation email. During the early morning hours, from 12 AM to 6 AM, the click frequency remains relatively low, ranging from 0.15% to 0.81%. This can be attributed to the reduced email activity during these hours, as users are less likely to be actively checking their inboxes before starting their workday. As the workday commences, one witnesses a gradual increase in click frequency, with peak engagement occurring between 8 AM and 11 AM. During this period, the percentage of clicks ranges from 7.23% to 9.92%. This finding aligns with the typical start of the working day when users are actively checking and responding to emails. The higher click frequency during these hours indicates an increased vulnerability to phishing attacks, as users may be more inclined to promptly interact with emails without thoroughly scrutinizing their authenticity. Throughout the midday hours, from 12 PM to 3 PM, the click frequency remains consistently high, ranging from 7.74% to 8.96%. This period coincides with lunch breaks, during which users often engage with their mobile devices, including checking personal and work emails. As the afternoon progresses, the click frequency gradually decreases, with percentages ranging from 4.40% to 3.18% between 4 PM and 7 PM. As the workday nears its end, users may be wrapping up their tasks and decreasing their engagement with work-related emails. Students, too, are likely finishing their classes for the day, leading to a decrease in email activity. Moving into the evening and nighttime hours, the click frequency further declines. From 8 PM to 11 PM, the percentage of clicks ranges from 2.60% to 0.86%.

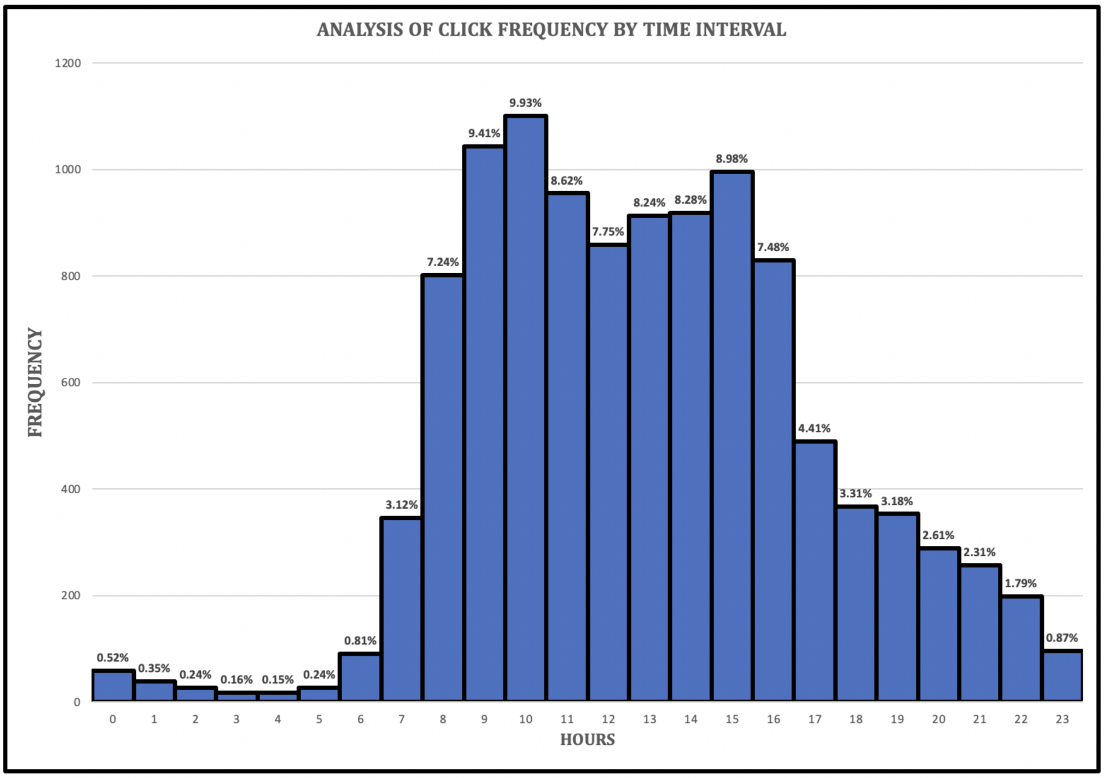


Figure 7: Analysis of Click Frequency by Time Interval in Phishing Simulation Campaign

7.3.5 Engagement on Education Landing Page

As highlighted in the interviews, the organization views the landing page as an educational opportunity for users, offering valuable information on how to recognize phishing emails, report incidents, and enhance their overall cybersecurity awareness. It offers insights into how users could have identified the phishing email and provides specific tips and tricks for enhanced awareness. Each box on the landing page highlights a particular aspect, such as checking email addresses, and includes an "Explain" button that users can click to delve deeper into the topic and gain a better understanding. Analyzing the data

(Figure 8), one can observe that the majority of users (69.49%) clicked on only one call-to-action (CTA) on the landing page. This might suggest a lack of active exploration and limited engagement with the educational content. As the number of clicks increases, the percentage of users decreases significantly, indicating a declining trend in user interaction with additional CTAs. For instance, only 20.80% of users clicked on two CTAs, followed by a gradual decline in engagement for higher numbers of clicks.

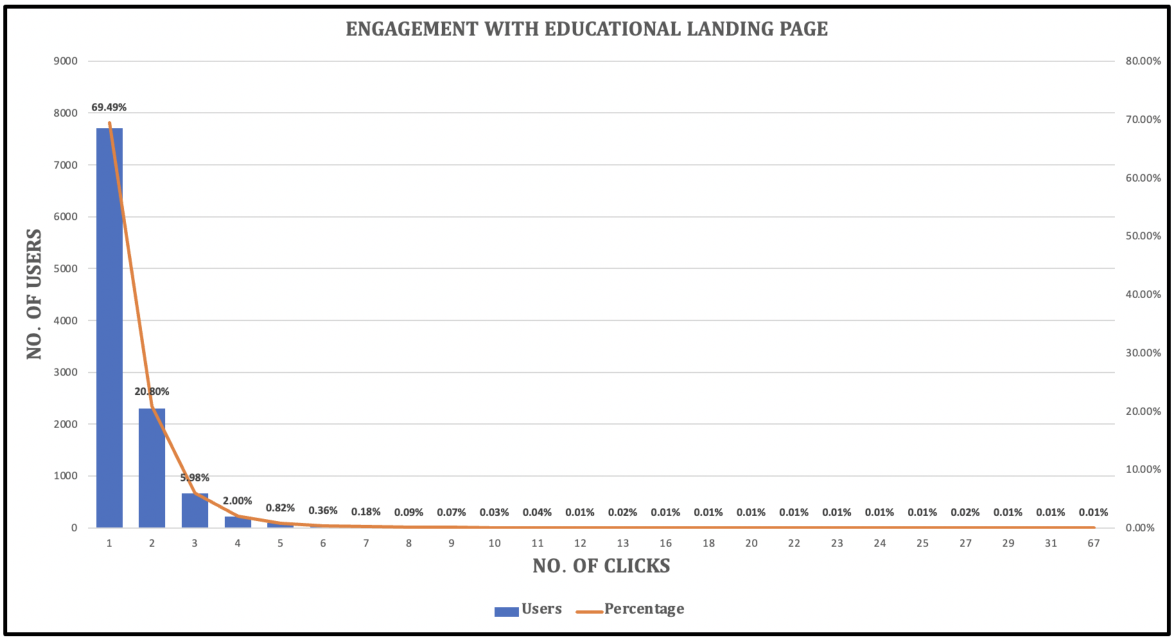


Figure 8: Analysis of Engagement on Education Landing Page based on Number of clicks

The low frequency of engagement with the content on the landing page raises concerns about the effectiveness of the educational content in capturing users' attention and fostering deeper engagement. Interviewee P8 also stressed on this by stating, *"what is funny to see is that the moment isn't actually the best learning moments. Because people are being pulled away from their work, they're doing some research, seeing an email, clicking on the link, and then they're distracted and they say, OK, I'm doing my job right now. So let's skip this. So that's not the perfect moment of training. Also, people are in a state of emotion. Somehow they feel like they're a bit fooled. So yeah, efficiency of the educational landing pages is to be doubted."* Considering these insights, it is important for the organization to reassess the landing page's effectiveness in terms of user engagement and learning outcomes. However, it is important to highlight some limitations of this data. Firstly, it assumes that users need additional information beyond the provided headers, but it's possible that some users understood the tips and tricks based solely on the headers themselves. Secondly, the analysis relies solely on click data and does not take into account other behavioral indicators such as time spent on the page or interaction with other elements.

7.3.6 Repeated Clickers

In this analysis (Table 4), the term "repeated clickers" refers to individuals who clicked on the links in both phishing simulation rounds. These individuals demonstrate a consistent pattern of engaging with potentially malicious content despite previous exposure to phishing awareness campaigns. According to the data collected, a total of 2,665 repeated clickers were identified across various user groups. Among them, the majority were students, accounting for 73.8% of the repeated clickers. Faculty members comprised 20.8% of the repeated clickers, while support staff represented 5.4%.

Table 4: Analysis of Repeated Clickers

User Groups	Number of Repeated Clickers	Percentage of Repeated Clickers	Percentage of Total Population
Student	1967	73.8%	6.79%
Faculty	555	20.8%	6.22%
Support Staff	143	5.4%	3.15%
Grand Total	**2665**	**100%**	**6.28%**

The presence of a considerable number of repeated clickers raises concerns about the effectiveness of the organization's phishing awareness and training programs. Despite exposure to prior simulations and educational initiatives, these individuals continue to fall victim to phishing attempts. The percentage of repeated clickers within the total population is an important metric to consider. Across all user groups, repeated clickers make up 6.28% of the organization's population. This indicates a notable proportion of individuals who exhibit a higher susceptibility to phishing attacks, thereby posing an elevated risk to the organization.

7.3.7 Reporting

Table 5 provides insights into the reporting numbers across the different user groups within the organization. Out of the total population of 42,417 users, 6.1% reported the simulated phishing attempt. Within the organization, where reporting rates serve as a metric to gauge awareness, the current reporting rate is considered relatively low. The organization encourages reporting during simulations as they believe it increases the likelihood that individuals will recognize and report real phishing attacks in the future. The organization considers this aspect crucial for its cybersecurity defense as it enables swift identification and mitigation of phishing threats.

Table 5: Phishing Simulation Round 2: Reporting Rates

User Group	Total Population	Users Reported	Percentage
Students	28,951	436	1.5%
Faculty & Support Staff	13,466	2174	16.1%
TOTAL	**42,417**	**2610**	**6.1%**

Examining the data across different user groups, it is observed that the reporting rate varies. Among students, 1.5% reported the phishing simulation, while faculty and support staff had a higher reporting rate of 16.1%. This suggests that faculty and support staff may be more vigilant or proactive in identifying and reporting phishing attempts compared to students. However, it is important to note that the organization's data does not provide a breakdown of the reporting rates specifically for faculty and support staff, as they are grouped together. This limitation restricts a more precise analysis of reporting behaviors within this specific user category.

7.4 Chapter Summary

This chapter aimed to examine the clicking and reporting behavior of users in response to phishing simulation campaigns. Before delving into the data analysis, the chapter provided insights into the steps taken to design the campaigns. The partner company employs social psychology principles and attempts to mimic the tactics used by cybercriminals when designing phishing simulation emails as showcased in 7.2. The metrics used for evaluation, such as the number of emails sent, click rates on links, and the number of emails reported, are consistent with industry standards. The frequency of campaigns, set at one every quarter, appeared to strike a balance between increasing awareness and not overwhelming the users. The analysis of click rates revealed that students and faculty members were the most susceptible groups within the organization. This highlights the importance of targeted awareness and training programs tailored to these specific user segments. Examining the time interval between email receipt and engagement, it was found that approximately 25% of the users who fell for the phishing email did so within the first hour. This situation poses a challenge for the organization as a significant number of users are susceptible to phishing attacks based on their response times, particularly during the initial hour if the phishing attempt goes undetected. Furthermore, the analysis of the time of day, when users clicked on the phishing simulation email link, revealed that users were more susceptible at the start of the working day when they were actively checking and responding to emails. Similarly, during lunch hours and the final hour before wrapping up for the day, users were more susceptible to phishing. These findings suggest that targeted awareness campaigns and heightened vigilance during these vulnerable time periods may be effective in reducing click rates.

The analysis of engagement on the educational landing page, specifically the number of clicks on elements that explained tips and tricks to identify phishing emails, indicated low engagement. This suggests that the current timing may not be the most effective educational moment. However, it is important to note that this data alone does not provide a conclusive understanding, as it does not account for other behavioral indicators such as the time spent on the page. The percentage of repeated clickers, individuals who fell for phishing attempts in multiple simulation rounds, stood at 6.28% across the organization. Students and faculty made up a significant portion of the repeated clickers and these findings suggest the need for continuous education and targeted interventions for these individuals to enhance their awareness and reduce their vulnerability. Lastly, the analysis of reporting rates indicated a concerning low rate among students, with only 1.5% reporting suspicious emails. Understanding the barriers and challenges faced by students in reporting such incidents is crucial for developing effective reporting mechanisms. In contrast, the combined reporting rate for support staff and faculty stood at 16.1%, suggesting a higher level of awareness and willingness to report among these groups. However, the organization's data does not distinguish reporting rates between faculty and support staff, limiting a more detailed analysis of reporting behaviors within this user category.

8 Email Characteristics

This chapter presents an analysis of reported phishing emails, focusing on key characteristics observed within a sample of emails reported during a time period. The objective of this analysis is to investigate various aspects of these phishing emails, including the utilization of persuasion techniques based on Cialdini's principles, the date and time of the emails, and their categorization by type (government, ecommerce, administrator, academic, individual). The purpose of this analysis is two-fold. Firstly, the analysis aims to compare the characteristics observed in reported phishing attempts targeted at the organization with the persuasion techniques employed in phishing simulation campaigns conducted by the organization. By examining these phishing attempts within the specific context of the organization, valuable insights can be gained into whether the organization's simulation campaigns effectively mimic the techniques used by real-world attackers. Additionally, by studying the patterns of date and time associated with reported phishing emails and identifying the types of organizations attackers attempt to mimic, the organization can enable users to exercise extra caution and take appropriate preventive measures to mitigate the risks associated with phishing attacks.

8.1 Data Collection & Analysis

For this analysis, a selective list of reported phishing emails was provided by the security team. The dataset consisted of emails reported between 1st March 2023 and 15th May 2023. It is worth noting that some emails were reported by multiple users, but only one instance of each unique email was included in the analysis. The approach employed in this study involved document analysis, where the content and characteristics of the emails were examined. It is important to acknowledge that the sample size of the reported phishing emails in this analysis is relatively small. The analysis focused on three key aspects of the reported phishing emails: persuasion techniques, date and time of the email, and the individual/type of targeted organization impersonated. By examining the utilization of persuasion techniques, such as those based on Cialdini's principles, insights into the psychological tactics employed by attackers could be gained. This understanding is vital for identifying effective social engineering strategies and enhancing user awareness and training programs. The analysis of date and time attributes aimed to uncover potential patterns or trends in phishing attempts, which can aid in the development of proactive defense measures. Categorizing the emails by type provided valuable insights into the specific domains or sectors targeted by attackers, enabling targeted countermeasures. By studying real-life examples, this analysis contributes to the development of targeted awareness programs, equipping users with practical knowledge and strategies to identify and mitigate phishing risks and facilitate the ongoing improvement of email security measures and increasing user awareness in the ever-changing landscape of cyber threats.

8.2 Findings

8.2.1 Persuasion Techniques

Based on the analysis of the phishing emails in the dataset (Appendix 14), the research observed the utilization of persuasion techniques based on Cialdini's principles (Figure

2). The findings, presented in Table 6, reveal that the authority principle was the most frequently employed technique, appearing in 75.00% of the phishing emails. Following closely was the scarcity principle, utilized in 45.00% of the cases. The consistency principle was present in 42.50% of the emails, while the liking principle was observed in 15.00% of the cases. The social proof principle appeared in 7.50% of the emails, and the reciprocity principle was identified in only 2.50% of the cases.

Table 6: Analysis of Persuasion Techniques in Reported Emails

CIALDINI'S PRINCIPLES	FREQUENCY	PERCENTAGE
Authority	30	75.00%
Scarcity	18	45.00%
Consistency	17	42.50%
Liking	6	15.00%
Social Proof	3	7.50%
Reciprocity	1	2.50%

The effectiveness of the authority principle suggests that individuals may be inclined to comply with requests from authoritative figures to avoid potential negative consequences. Additionally, the prevalence of the scarcity principle indicates that phishers leverage the perception of limited availability to create a sense of urgency or fear of missing out (FOMO) among recipients. It is important to note that these persuasion techniques are not mutually exclusive, as a single phishing email may employ multiple principles simultaneously. Hence, the total percentage does not sum up to 100%. The significance of authority and scarcity as prevalent techniques underscores the importance of enhancing user awareness and understanding of these specific tactics employed by phishers. Such insights contribute to a deeper comprehension of the strategies used in phishing attacks and aid in the development of more effective countermeasures to protect individuals and organizations from falling victim to these attacks.

8.2.2 Target Types

The analysis of the phishing emails in the dataset, as shown in Table 7, aimed to examine the target types impersonated by attackers (Figure 15). Among the different target types , the most commonly impersonated were "Individual" and "Financial," each accounting for 22.5% of the phishing emails. For instance, attackers targeted individuals by posing as professors and sending emails to colleagues, while others exploited financial matters, such as fake invoices, gift card scams, and activation links of bank accounts. These examples demonstrate the attackers' exploitation of personal connections and financial motivations to increase the success rate of their phishing attempts.

Another prominent target type identified in the analysis was "Administrator" appearing in 17.5% of the phishing emails. Phishers strategically impersonated administrators, such as the President of the organization, or claimed to be from the helpdesk department, creating a sense of authority and legitimacy. By leveraging positions of authority, attackers aimed to deceive recipients into complying with their requests. Additionally, the analysis revealed that "Government Authority" was targeted in 15.0% of the phishing emails. In multiple cases, attackers impersonated the Chamber of Commerce (KVK) and used deceptive tactics, such as QR codes, to trick recipients into divulging sensitive information.

The targeting of "E-Commerce" and "Academic" entities constituted 10.0% and 7.5% of the phishing emails, respectively. Phishers used various techniques, such as claiming orders from popular retailers like Walmart or sending attachments related to academic research papers. Lastly, 5.0% of the phishing emails targeted "Telecommunication" entities. Attackers impersonated mobile service carriers, like AT&T, and created a sense of urgency by claiming that voicemails would expire soon. These phishing emails often included attachments that potentially contained malicious content.

Table 7: Analysis of Target Types Impersonated in Reported Emails

TARGET	**FREQUENCY**	**PERCENTAGE**
Individual	9	22.5%
Financial	9	22.5%
Adminstrator	7	17.5%
Government	6	15.0%
E-Commerce	4	10.0%
Academic	3	7.5%
Telecommunication	2	5.0%
TOTAL	**40**	**100.0%**

8.2.3 Day and Timing Analysis

The analysis of the phishing emails presented in Table 8 reveals interesting patterns regarding the days on which attackers choose to send their malicious messages. The findings demonstrate a notable preference for phishing email distribution on Mondays, which accounted for 30.0% of the dataset. This suggests that attackers capitalize on the start of the workweek, taking advantage of increased email traffic and potential distractions that may accompany individuals' return to work after the weekend. Following closely behind, Fridays emerged as the second most common day for phishing email distribution, representing 25.0% of the dataset. Attackers may target Fridays, anticipating a potential decline in individuals' focus and vigilance as the workweek draws to a close. Thursdays and Wednesdays each accounted for 15.0% of the dataset, while Tuesdays represented 10.0%. These findings suggest While there is a notable concentration of phishing emails on Mondays and Fridays, it is important to recognize that attackers distribute phishing emails consistently throughout the workweek.

Table 8: Day of the Week Analysis of Reported Emails

DAY	**FREQUENCY**	**PERCENTAGE**
Monday	12	30.0%
Friday	10	25.0%
Thursday	6	15.0%
Wednesday	6	15.0%
Tuesday	4	10.0%
Sunday	2	5.0%
TOTAL	**40**	**100%**

The timing analysis of phishing emails presented in Table 9 reveals interesting patterns regarding the preferred hours for sending such malicious emails. The interval between 12:00 PM and 3:59 PM emerges as the peak period for phishing email distribution, accounting for 27.5% of the dataset. This concentration suggests that attackers strategically exploit these midday hours when individuals are heavily engaged in work-related tasks and communication. Notably, this timeframe also coincides with the lunch break for many individuals. The hours from 8:00 AM to 11:59 AM also exhibit a significant concentration of phishing emails, accounting for 25.0% of the dataset. This time period marks the start of the workday, where individuals may face a backlog of emails and prioritize addressing their inbox promptly. Attackers may exploit this situation, recognizing that individuals are likely to be focused on catching up with their tasks and may have a higher vulnerability to phishing attempts during this time. Between 4:00 PM and 7:59 PM, there is a slightly reduced frequency of phishing emails, constituting 17.5% of the dataset. The interval between 4:00 AM and 7:59 AM corresponds to the early hours of the day and accounts for 15.0% of the phishing emails. These early-morning phishing emails

Table 9: Analysis of Timing of Reported Emails

TIMING	FREQUENCY	PERCENTAGE
12:00 PM - 3:59 PM	11	27.5%
8:00 AM - 11:59 AM	10	25.0%
4:00 PM - 7:59 PM	7	17.5%
4:00 AM - 7:59 AM	6	15.0%
8:00 PM - 11:59 PM	4	10.0%
12:00 AM - 3:59 AM	2	5.0%
TOTAL	**40**	**100%**

potentially have a higher chance of being the first thing individuals view when checking their inbox. The evening timeframe from 8:00 PM to 11:59 PM represents 10.0% of the phishing emails. Although the frequency is relatively lower during these hours, attackers still target this period. Lastly, the interval between 12:00 AM and 3:59 AM has the lowest frequency of phishing emails, accounting for 5.0% of the dataset. The lower concentration of phishing emails during late-night and early-morning hours may be attributed to individuals being offline or experiencing reduced email activity. This, coupled with the uncommonness of work-related emails during these hours, suggests that attackers may find fewer opportunities and individuals may exercise greater caution.

8.3 Comparison with Phishing Simulation Emails

The analysis carried out on the phishing simulation emails sent during the three rounds aims to evaluate their effectiveness in incorporating persuasion principles observed in reported phishing attempts. The first simulated phishing email (Figure 16), posing as a Microsoft administrator, utilized the principles of scarcity and authority. It created a sense of urgency by emphasizing the expiration of the activation link at the end of the month, while also leveraging the credibility associated with Microsoft. The second email (Figure 17), mimicking the IT department, employed the principles of authority, scarcity, and consistency. It notified users of upcoming password expiration, invoking the authority of the IT department and using a three-day time limit to create a sense of urgency. The email is also consistent with security practices of the organization as users are required to periodically change their password. Lastly, the third email (Figure 18), posing as the IT service desk, also capitalized on the principles of scarcity and authority. It generated urgency by warning of full account storage and the potential loss of email functionality. The authoritative position of the IT service desk added credibility to the email's claims.

By comparing the organization's phishing simulation emails with the common persuasion techniques observed in reported phishing attempts (Table 6), it becomes evident that the organization has successfully replicated the most prevalent tactics employed by attackers. The simulations utilize authority and scarcity in all emails, and consistency is employed in the second email. This strategic approach creates a realistic environment for users to enhance their skills in identifying and responding to phishing attacks. The incorporation of these elements provides valuable training opportunities by empowering users to better recognize and mitigate actual phishing threats. As seen in Table 7, around 50% of the reported phishing attempts occurred between 8 PM and 4 PM. Comparing this to the click behavior by time intervals of the second phishing simulation round, around 75% of the users that clicked the phishing emails clicked it between 8 AM and 4 PM. This pattern suggests that attackers take advantage of users' active engagement with their work emails during this time, making them more vulnerable to phishing attacks. By exploiting the users' focused attention and potential distractions, attackers increase the likelihood of their phishing emails being successful. It is crucial to acknowledge this strategy and raise awareness among users about the increased risks during these periods.

8.4 Chapter Summary

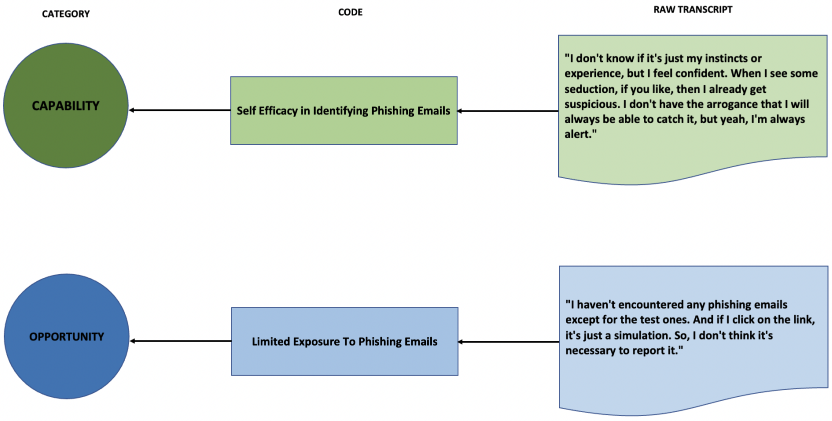
This chapter aimed to provide an analysis of the characteristics and persuasion techniques used in reported phishing emails and assess whether the phishing simulation emails effectively replicate characteristics and techniques. The findings revealed that the most prevalent persuasion techniques in reported phishing emails were the authority and scarcity principles. These techniques were successfully replicated in the phishing simulation emails conducted by the organization. By incorporating these elements into the simulations, users were exposed to realistic scenarios that aimed to enhance their skills in identifying and responding to sophisticated phishing attacks. Additionally, the analysis identified various target types, with individuals, financial entities, and administrators being the most commonly impersonated. Attackers strategically exploited personal connections, financial motivations, and positions of authority to exploit users and increase the likelihood of falling for phishing attempts. Moreover, the analysis examined the distribution patterns of phishing emails and identified the most common days and times for attackers. The findings revealed that Monday and Friday accounted for over 50% of the observed phishing attempts, while the majority of attempts (over 50%) occurred between 8 AM and 4 PM. In comparison to the click behavior observed during the second phishing simulation round, it was notable that a significant majority (around 75%) of users who engaged with the phishing emails did so between 8 AM and 4 PM. This pattern suggests that attackers strategically target users during their busy work schedules or towards the end of their workday when they may be more susceptible to falling for phishing attempts. The above analysis can help users identify and respond to malicious emails, thereby raising awareness and promoting a proactive approach to combat phishing attacks. By identifying the peak periods of phishing engagement, the organization can encourage users to exercise extra caution and remain vigilant during those times, enhancing their ability to detect and report suspicious emails. Furthermore, incorporating this analysis into awareness programs can provide engaging material that educates employees about the specific risks they may face during their busy work schedules. Finally, closely monitoring the network and system during these identified high-risk periods allows the organization to implement proactive measures and swiftly respond to potential phishing attacks, safeguarding its infrastructure and data.

9 User Perspective

This chapter delves into the findings derived from semi-structured interviews conducted with users representing various user groups, including students, faculty, and support staff. The primary objective of this chapter is to gain insights into the factors that influence users' reporting behavior in phishing incidents. Additionally, the chapter aims to extract recommendations provided by the users regarding how the organization can improve its infrastructure and support systems to foster a reporting culture. To structure and present the findings in a comprehensive manner, the COM-B model is employed as a framework. This model provides a multidimensional perspective, encompassing the capabilities, opportunities, and motivations that shape users' reporting behavior. By analyzing and synthesizing these findings, the chapter will provide valuable insights and practical recommendations for enhancing the organization's reporting infrastructure and support systems, thus strengthening its overall cybersecurity defenses.

9.1 Data Collection and Interpretation

In order to gather insights into the factors influencing users' reporting behavior in phishing incidents and obtain recommendations for improving the organization's infrastructure and support systems, a total of 26 interviews were conducted with users from various groups, including students, faculty, and support staff. Among these interviews (Figure 10), 16 were conducted via Teams, while 8 were conducted in person. Prior to the interviews, participants were asked to sign an informed consent form, either written or orally, which ensured the confidentiality and anonymity of the data. All participants granted permission for the interviews to be recorded for reference purposes. The interviews had an average duration of 21 minutes, with the shortest interview lasting 16 minutes and the longest lasting 34 minutes. The analysis of the qualitative data collected from the user interviews was conducted using a thematic analysis approach. The thematic analysis involved a deductive coding process (Figure 9), utilizing the pre-defined framework of the COMB model, which encompasses the categories of Capability, Motivation, and Opportunity. This coding process allowed for a systematic examination of the interview data, identifying relevant excerpts and categorizing them into the respective categories as outlined by the model.

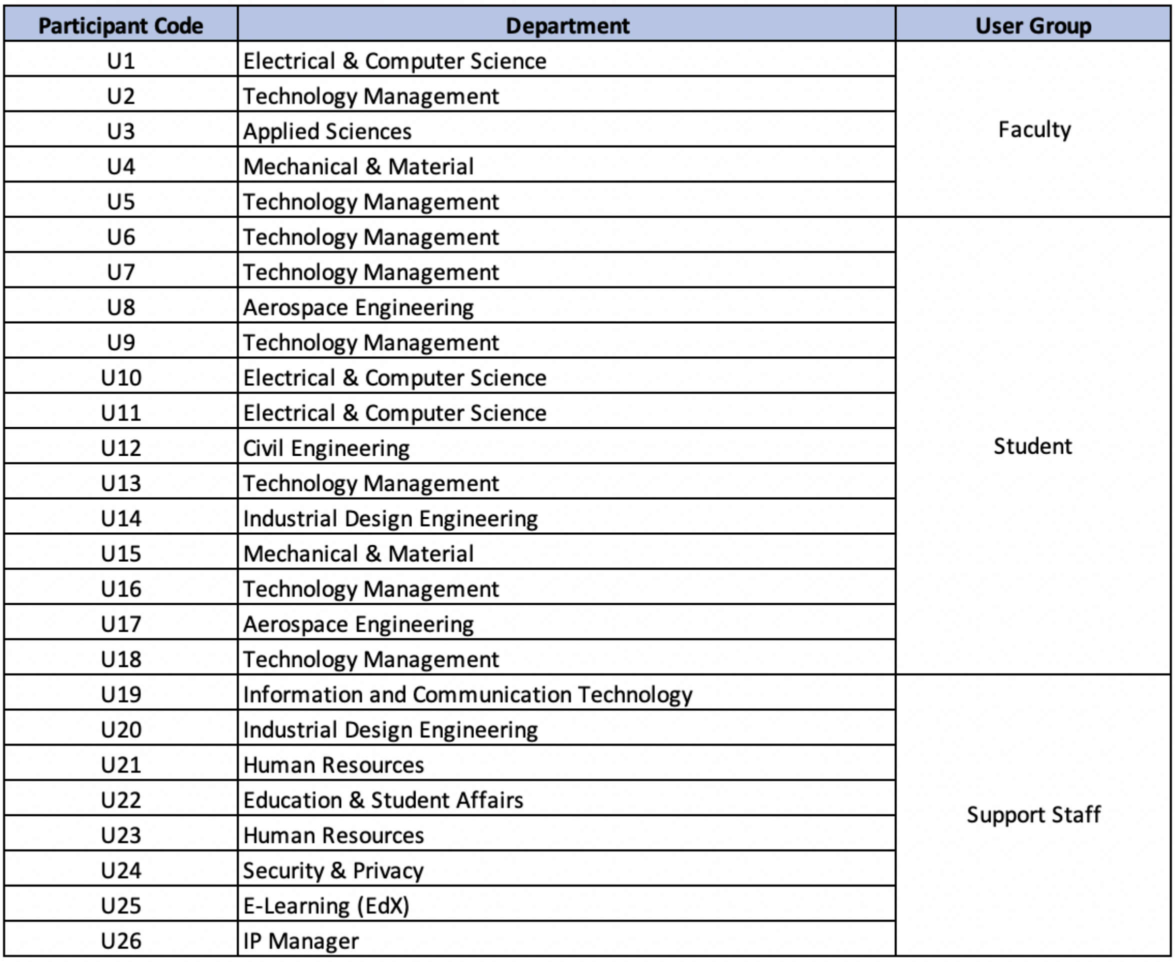


CATEGORY
CODE
RAW TRANSCRIPT
CAPABILITY
Self Efficacy in Identifying Phishing Emails
OPPORTUNITY
Limited Exposure To Phishing Emails

"I don't know if it's just my instincts or experience, but I feel confident. When I see some seduction, if you like, then I already get suspicious. I don't have the arrogance that I will always be able to catch it, but yeah, I'm always alert."

"I haven't encountered any phishing emails except for the test ones. And if I click on the link, it's just a simulation. So, I don't think it's necessary to report it."

Figure 9: Deductive Coding Example



Participant Code	Department	User Group
U1	Electrical & Computer Science	Faculty
U2	Technology Management	
U3	Applied Sciences	
U4	Mechanical & Material	
U5	Technology Management	
U6	Technology Management	Student
U7	Technology Management	
U8	Aerospace Engineering	
U9	Technology Management	
U10	Electrical & Computer Science	
U11	Electrical & Computer Science	
U12	Civil Engineering	
U13	Technology Management	
U14	Industrial Design Engineering	
U15	Mechanical & Material	
U16	Technology Management	
U17	Aerospace Engineering	
U18	Technology Management	
U19	Information and Communication Technology	Support Staff
U20	Industrial Design Engineering	
U21	Human Resources	
U22	Education & Student Affairs	
U23	Human Resources	
U24	Security & Privacy	
U25	E-Learning (EdX)	
U26	IP Manager	

Figure 10: Overview of User Interviewees

9.2 COM-B Model

The study adopts the COM-B model (Capability, Opportunity, Motivation, and Behavior) as a theoretical framework to investigate the factors influencing reporting behavior in phishing incidents. The COM-B model provides a comprehensive perspective by examining the interplay of users' capabilities, opportunities, motivations, and resulting behaviors in the context of cybersecurity. Capability encompasses users' knowledge, skills, and awareness of phishing threats and their potential consequences. Opportunity refers to the contextual factors and organizational infrastructure that facilitate or hinder reporting behavior. Motivation encompasses the individual's inclination, perceived benefits, and perceived risks associated with reporting phishing incidents. The subsequent sections will provide a detailed analysis and discussion of the findings within each category of the COM-B model shedding light on the factors influencing users' reporting behavior in the context of phishing.

9.2.1 Capability

The analysis of the capability aspect within the COM-B model (Figure 11) sheds light on the users' proficiency, knowledge, and confidence in recognizing phishing emails, while also exploring their understanding of the potential repercussions of phishing attacks. The findings from the interviews with both users who have reported phishing incidents and those who haven't shed light on these factors highlighting the variations in capability among different user groups. Users who have reported phishing emails demonstrated a higher sense of self-efficacy in their ability to identify and report suspicious emails. *"I don't know if it's just my instincts or experience, but I feel confident. When I see some seduction, if you like, then I already get suspicious. I don't have the arrogance that I will always be able to catch it, but yeah, I'm always alert." [U23]* The confidence exhibited by users in identifying phishing emails can be attributed to their exposure to a significant number of such emails - *"ohh well I get a lot of them, so by now I'm used to them. They're mostly similar in their style as well, and I'm like, OK guys, this is not working." [U20]* However, users also raised concerns about the increasing sophistication of these emails which might hamper their ability to identify them. This was highlighted by Interviewee U3, *"well, in the past it was obvious because you could see the sender's address, you could see spelling errors, you could see lots of things that were a mismatch. Now they become more evolved, so it is becoming harder."* Participants also expressed their concern about potentially flagging legitimate emails as phishing and highlighted the need for caution. As one participant stated, *"Yea, when in doubt, I forward it to my manager first to confirm as some emails can be relevant for the other teams we work with." [U25]*

On the other hand, users who haven't reported phishing incidents expressed lower levels of confidence in their ability to identify phishing emails. Some participants mentioned falling for the phishing simulation emails, which undermined their confidence in distinguishing legitimate emails from phishing attempts: *"I must admit, I fell for the storage full email a few weeks ago and that made me doubt whether I can identify those emails. But then, these emails are trickier than ones I have received on my personal email. The password reset one was also tough because my password was actually expiring around the same time." [U17]* The sentiment regarding the sophistication and difficulty of phishing simulation emails was echoed by several participants, highlighting the impact it has on user confidence. Participant U19 emphasized the importance of starting with less sophisticated phishing emails, stating, "*Having said that, I think it's also good to start with a little bit less sophisticated phishing emails...A lot of people will fall for these and it can get demotivating for people.*"

The participants' understanding of the potential consequences of phishing attacks on the organization varied among users. Users who have reported phishing emails demonstrated a strong awareness of the potential consequences, particularly related to the data they handle based on their job roles: *"The consequences on the organization can be huge as getting into the patent database would be highly interesting for certain companies and governments. Quantum computing, nuclear research, this is stuff they would like to have." [U26]* The potential consequences related to data confidentiality, reputational damage, system lockouts, and financial losses to the university were commonly mentioned by these users. The findings indicate that users' awareness of the potential consequences plays can impact their reporting behavior. Recognizing the potential harm that phishing attacks can cause to the organization's valuable data and overall operations, users who possess a deeper understanding of these potential consequences are more inclined to report suspicious emails.

In contrast, users who haven't reported phishing incidents displayed a lesser understanding of the potential consequences of such attacks. They cited limited exposure to real-life examples or situations, leading to a lack of awareness. One user candidly admitted, *"To be honest, I'm not so aware or worried about the consequences regarding the university. Most of the personal data they have is my grades, so I'm more concerned about phishing emails related to my personal email account." [U10]* This suggests that the lack of awareness of the potential consequences of phishing attacks on the organization can impact users reporting behavior as users may overlook that their university email accounts grant access to the directory of all email IDs registered within the organization, potentially exposing other users to risks if the directory is compromised. Additionally, research data, communication with colleagues/faculty, and sensitive information shared via email are examples of content that users may not want to be compromised. One participant also mentioned how *"sometimes there is privacy-sensitive content on my email. Let's say. I mean, could be anything about mental health or family problems or I mean, doesn't happen so often, but it happens." [U2]* Similarly, a few participants expressed the view that deleting or ignoring suspicious emails served as an alternative to reporting. Notably, they were unaware of the importance to report such incidents and the role reporting plays in safeguarding the organization. Although this behavior demonstrated their capability in recognizing and protecting themselves, it also revealed a gap in their understanding of the broader impact of reporting on organizational protection.

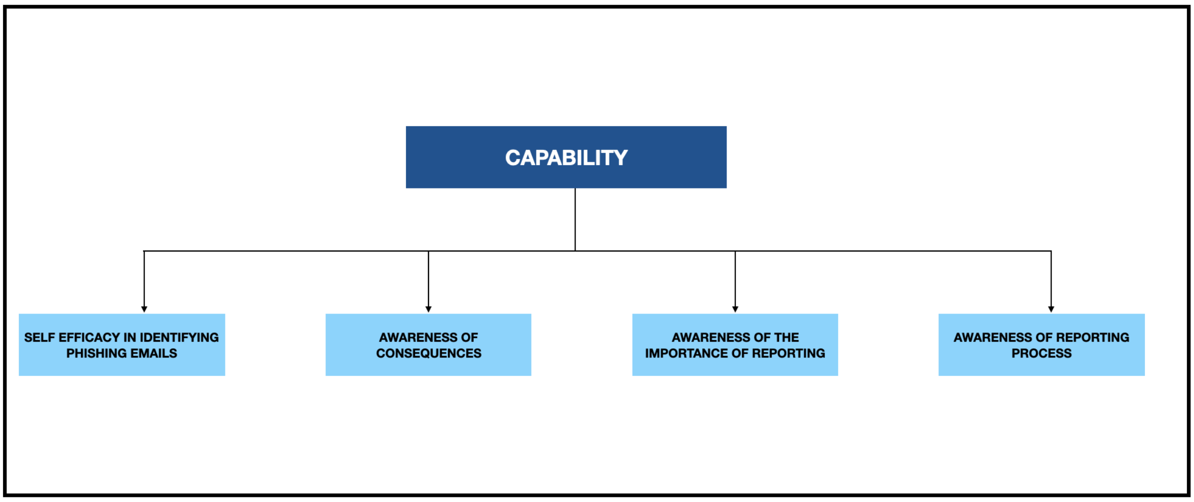

CAPABILITY
SELF EFFICACY IN IDENTIFYING PHISHING EMAILS
AWARENESS OF CONSEQUENCES
AWARENESS OF THE IMPORTANCE OF REPORTING
AWARENESS OF REPORTING PROCESS

Figure 11: Factors Influencing Reporting Behavior categorized under Capability

9.2.2 Opportunity

The opportunity section of the COM-B model (Figure 12) provides insights into external factors that influence users' reporting behavior. One common theme mentioned by both users who have reported and not reported was the importance of clarity in the reporting process. A majority of the users who have never reported before mentioned they weren't aware of the reporting process: *"I'll be honest, I don't know where to report and who handles it. In my previous organization, there was a button, but I don't see that here." [U6]* This highlights the need for clear and easily accessible information regarding the reporting process to ensure users are well-informed and empowered to take appropriate action. Interestingly, even users who have been reporting incidents shared their initial struggles in finding the correct email address to report phishing emails. One user shared their experience, stating, *"The thing is, I've been working here for a long time and I still had the previous email address where we had to report emails in my mailbox. And that's not the email address anymore...So I still used the old one to report, and then you think, God, I'm never gonna get a reply. And then you have to go somewhere to look for the information. And that's a bit annoying." [U22]*

Users who have reported incidents generally find the reporting process to be efficient and not excessively time-consuming. Participant U1 stated, *"It's really easy and takes 2 seconds. Press forward to abuse and then done. I think it's like the lowest level of hassle. I'm very glad that they didn't imagine some ticketing system to do this. I would never submit anything"*. Most of these users feel that reporting incidents does not significantly disrupt their workday. The majority of them attributed this to repetition and their experience of having been doing it for a long time. They acknowledged that as they became more familiar with the process and encountered phishing attempts regularly, it became more of a routine task integrated into their daily workflow. However, even among users who have reported, there were a couple of concerns about the potential time and effort required, especially on busy days: *"I worry that I might forget to report if I have too many things to do." [U21]* Similarly, a few users who haven't reported incidents voiced their concerns about the time-consuming nature of thoroughly scanning and reporting emails, especially when they are already overwhelmed with their workload. Participant U16 stated, *"Especially when I have deadlines and stuff, spending time on scanning emails and then reporting it isn't my priority."* Participants also mentioned that timely acknowledgment and feedback influences reporting behavior - "*if there's no feedback, so it's like, what's the purpose? You never know. What you do it for?" [U5].* When users receive prompt acknowledgment and feedback, they feel their efforts are valued, fostering a sense of involvement and encouraging continued reporting. Some participants also highlighted the role of their colleagues in promoting reporting behavior: *"You know, we also alert each other, like someone receives an email, puts it in our team's group...I think that's also very helpful. So it's not borne by one person." [U23]*

Another factor that was mentioned across the interviews was the exposure to phishing emails. A significant number of users who haven't reported phishing incidents mentioned that they haven't come across any phishing attempts apart from the simulated ones sent by the university: *"I haven't encountered any phishing emails except for the test ones. And if I click on the link, it's just a simulation. So, I don't think it's necessary to report it." [U12]* This limited exposure to real phishing emails reduces their opportunities to report such incidents. It is worth noting that this may indicate the effectiveness of the email filters in successfully detecting and blocking phishing attempts. Among the users who correctly identified the simulated phishing emails and reported them, a couple of them expressed dissatisfaction with the repetition of such exercises. They indicated that they might not participate in future simulations due to this reason. However, for a majority of the users who have reported multiple times, their continuous exposure to phishing attempts is a result of the nature of their work. Users in departments such as HR, Intellectual Property, and Student Affairs emphasized encountering phishing attempts more frequently. This indicates that their roles and responsibilities make them more susceptible to targeted phishing attacks.

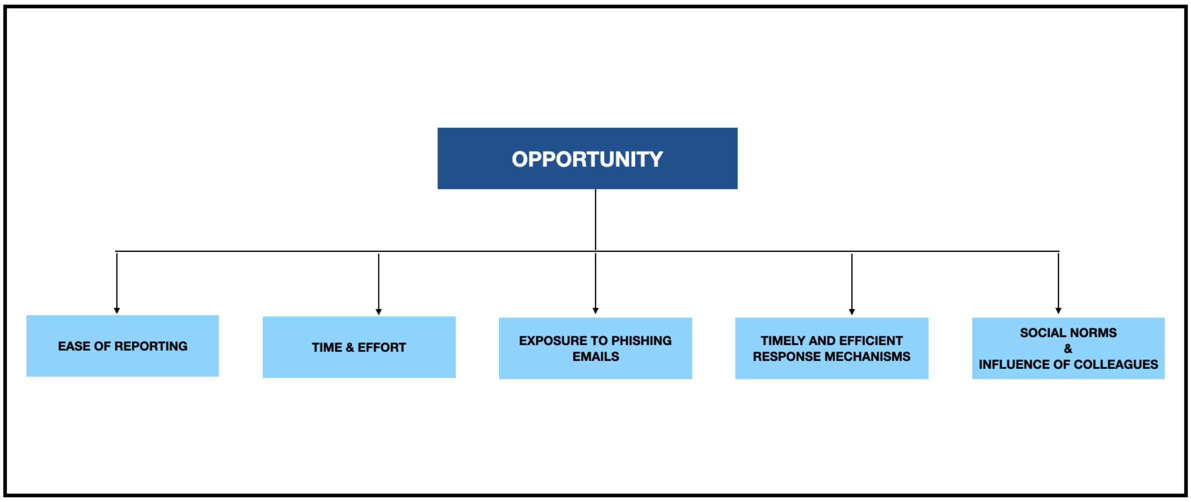

OPPORTUNITY
EASE OF REPORTING
TIME & EFFORT
EXPOSURE TO PHISHING EMAILS
TIMELY AND EFFICIENT RESPONSE MECHANISMS
SOCIAL NORMS & INFLUENCE OF COLLEAGUES

Figure 12: Factors Influencing Reporting Behavior categorized under Opportunity

9.2.3 Motivation

The analysis of the motivation aspect within the COM-B model (Figure 13) showed that for many individuals, reporting phishing incidents is driven by intrinsic motivation and personal work ethic and values. They view it as an extension of their character and a reflection of their commitment to doing the right thing. As one user aptly put it, *"I think that's a personality trait. If I see a piece of paper on the street, I pick it up and put it in the bin. That's the way I work. So that's my motivation. I think it's good work ethic."[U4]* This natural inclination to take action and contribute to a safe environment extends to their digital behavior, where they actively identify and report phishing attempts.

Another important factor that influences users' motivation to report phishing incidents is their collective responsibility towards their colleagues and the community as a whole. They recognize that reporting these incidents is not solely about protecting themselves, but also about safeguarding others. This collective responsibility is driven by a genuine concern for their colleagues' well-being and a shared commitment to the organization's security. As one user highlighted, *"I wouldn't want to say responsibility, but for the organization and for my colleagues, as in, I recognize this. I would want somebody else that recognizes this to report it for me on the off chance that I may be misled. So it's maybe for the greater good, I don't know." [U1]* This perspective reflects an understanding that individual actions can have a ripple effect, and by actively reporting phishing attempts, they contribute to protecting the university against cyber threats. Even among users who haven't reported phishing incidents, many still acknowledge the shared responsibility of keeping the university safe. While they rely on the IT team to establish protective measures, they understand that they too have a part to play in maintaining security. As Participant U3 mentioned, *"Yea in a sense I think it is the IT teams responsibility to protect the university by blocking these emails. But then yea ofcourse, they cannot block everything, as someone will find a loophole and then we are responsible in a certain way."* While both participants from the ICT team viewed reporting as a part of their job responsibilities, it was interesting to hear a couple of other participants view this as a part of their job as well: *"OK, well for me, just like the safety of the systems and our data, I feel like it's a part of my job and me being like a responsible employee." [U20]*

The interviews also revealed personal experiences or knowing someone who has fallen victim to a cyberattack also influence users' motivation to report phishing incidents. Three participants mentioned they had witnessed the adverse effects of phishing first-hand through stories shared by others. They understand the importance of reporting and preventing similar incidents from occurring: *"I recall one of the experiences from my bachelors in another institute where one of my friends who was an international student got an e-mail from the university account stating that she had to pay a huge amount of money as her tuition fee and without checking the validity, she paid the money. This was sent to multiple students and after this experience I realized if someone would have told the authorities, she wouldn't have lost that money." [U19]*

Another factor that came to light was that the perceived threat of an email also influences reporting behavior. While users may often overlook or dismiss more obvious phishing attempts, they exhibit a higher likelihood of reporting emails that they perceive as targeted and carrying a greater risk. As Participant U22 shared, "*When you receive those 'we have somebody dying in that country and you're the only relative' or 'you're the person that gets all their money' scams, those are easy to spot. But a few months ago, I received an email from T-Mobile, supposedly from our organization's suppliers, asking me to click links and log in. So those are more dangerous and I immediately reported it.*" This highlights how users differentiate between different types of phishing emails based on their perceived threat levels, prioritizing the reporting of more targeted and sophisticated attempts.

A few participants also raised concerns regarding the perceived effectiveness of reporting and how their actions contribute to the organization's protection. As one user highlighted, *"Like I have no idea if it is worth reporting these emails or if reporting the mail, in general, has any outcome." [U10]* This highlights the need for the organization to provide clearer communication and feedback to users regarding the outcomes of their reports. Users want to know if their reports are making an impact and if measures are being taken to enhance overall security based on their contributions. This opinion was also shared by multiple users who reported emails in the past but did not receive any feedback on the actions taken or impact of the report. Lastly, one participant also raised concerns about the privacy of data during the phishing simulation emails. The organization partners with another company for the phishing simulation exercises and the participant wasn't too pleased as they remarked, " *"The first time I reported and then the second and third the second time I still reported and say ohh. It's just a test. La La, la, la, la and then the third time I started to ignore it and then I start to complain about it to exclude me from these tests. Because I hated that they provide my data to a 3rd company" [U3].* This experience highlights the importance of maintaining user privacy and ensuring clear communication when conducting phishing tests or any other security-related activities.

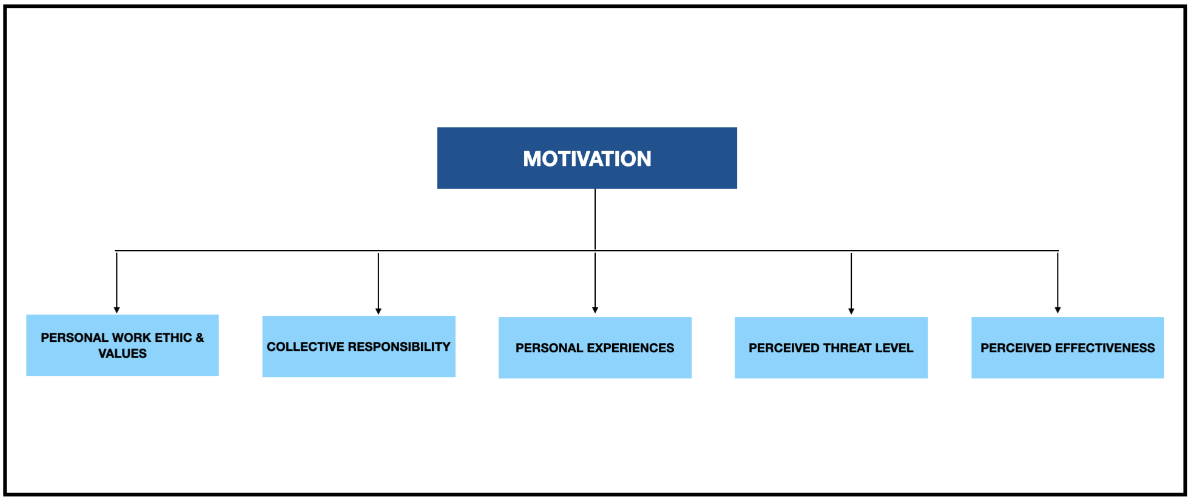


Figure 13: Factors Influencing Reporting Behavior categorized under Motivation

9.3 Infrastructure & Support Enhancement

In addition to gaining insights into factors that influence reporting behavior, the interviews also provided valuable recommendations for enhancing the organization's infrastructure and support systems. These recommendations have been categorized into three key areas: educational measures, reporting process, and incentives.

9.3.1 Educational Measures

A considerable number of participants expressed concerns about the lack of awareness regarding phishing attacks and believe training programs would be beneficial. They mentioned their openness to such programs during the onboarding process and at the start of the academic year.: *"I think on the matter of introduction for new personal, if I related to myself, I haven't had any IT introduction at all. This can be improved I think, just for new people to be able to know about security processes or how to identify phishing emails or where to report and stuff." [U24]* However, participants also highlighted the need for the organization to exercise caution in their communication strategies for these training programs with clear and effective communication deemed essential to ensure user participation. They also highlighted the importance of designing training programs that are worthwhile and engaging: *"It should be something interesting that actually makes people want to learn, not just a dull lecture. Back in my previous organization, in these trainings and you would just go click, click, click, click through and people were really ranting about* *that." [U26]*

Participants stressed on the importance of sharing real-life examples and consequences of phishing attacks as an effective educational approach. By showcasing actual instances of how individuals and organizations have been harmed by phishing incidents, users gain a better understanding of the risks involved. Participant U10 expressed this sentiment stating, *"Whenever these huge data breach scandals and what they really did with the data, then all of a sudden everyone was like, wow, how did that happen? So I think these examples are basically a little bit like the pictures on the cigarettes, you know, it's like maybe have this big example of what can happen and people may think about it a little bit further and take action in the future."* These firsthand accounts serve as cautionary tales that create a sense of urgency and highlight the critical need to remain vigilant in identifying and reporting phishing attempts.

Phishing simulations emerged as a widely recognized and effective method for raising awareness among participants. The majority of users expressed their belief in the value of these simulations, considering them valuable tools for educating users: *"I think the simulations are really effective. They are a real test and it keeps us on our toes." [U11]* The simulations were seen as a practical way to test and improve users' ability to identify and report phishing attempts. However, it is worth noting that a few participants voiced their dissatisfaction with the frequency of these simulations, perceiving them as excessive and intrusive. Despite this, there was a mixed response when it came to the frequency of the simulations, with some users expressing a desire for more frequent simulations to reinforce their vigilance, while others felt the current frequency was sufficient.

Alongside the training programs and phishing simulations, participants also recommended a dedicated website that provides comprehensive information on phishing and the latest trends and examples. This website would serve as a valuable resource to educate users about common phishing techniques, emerging threats, and real-life examples of successful and attempted phishing attacks. However, when participants were asked about their awareness of the existing Security and Privacy website, the findings revealed that the majority, with only two exceptions, were unaware of its existence. This lack of awareness indicates a significant communication gap and highlights the importance of improving the visibility and accessibility of the organization's Security and Privacy website: *"Having a website with up-to-date information and resources would be really helpful [U19]"*

9.3.2 Reporting Process

Participants suggested improvements to the reporting process to make it more efficient and effective. The implementation of a dedicated report button within the email client or other communication platforms was seen as a valuable addition. Participants who have reported before expressed enthusiasm for the addition of a dedicated report button, seeing it as a valuable enhancement to streamline and expedite the reporting process: *"So yeah, the best thing for me is just make sure there's a reporting button on the ribbon of your e-mail and then you can just click on report and send it in directly to the security team" [U19].* In the absence of a dedicated reporting button, participants expressed the need for the organization to periodically educate and communicate the reporting process to users.

It was evident that many participants were unaware of how to report phishing attempts. Therefore, regular reminders and updates regarding the reporting process are essential to ensure that all users are well-informed and equipped to report suspicious emails effectively.

Another important improvement suggested by participants is the provision of meaningful feedback after reporting. Participants expressed the importance of receiving confirmation regarding the legitimacy of their reported emails and whether their reports had contributed to identifying actual phishing attempts. Additionally, they highlighted the need for informative guidance and tips on how to handle similar situations in the future. Participants believed that receiving such feedback would not only address their concerns about the effectiveness of their reports but also increase their confidence in identifying such emails in the future. As participant U5 stated, "*It is important to receive some kind of answer related to whether the reported email is legitimate or not. Otherwise, you don't have a clue if what you have done has any kind of positive contribution. And you can also learn from it yourself.*" Additionally, while participants understood the need for automated acknowledgment messages, some raised concerns about the lack of informative responses to their specific questions. They felt that the automated messages did not sufficiently address their queries, leading to frustration and a sense of unresponsiveness. Participants emphasized the importance of providing informative and tailored responses to address their concerns effectively.

9.3.3 Incentives

Participants acknowledged the potential benefits of incentives in motivating individuals to report phishing incidents but suggested that reporting behavior should not solely rely on incentives. They expressed the belief that the reporting behavior should remain centered around protecting themselves and the organization, rather than being driven solely by incentives. Striking a balance is necessary to ensure that the main activities and responsibilities of the organization are not overshadowed or detracted from.

The majority of participants expressed the belief that an encouraging acknowledgment, such as a personalized message highlighting the user's contribution to keeping the university safe, would be a meaningful form of recognition. They mentioned that making the acknowledgment memorable and impactful for the user would further encourage reporting behavior. Suggestions included sending emails with stickers, GIFs, or other visually engaging elements, as well as personalizing the acknowledgment to make it feel more genuine and encouraging. Participants believed that such personalized acknowledgments would not only reinforce a positive reporting culture but also create a lasting impression that stays with the user: *"It's a bit childish but like what you get from saving water or energy, you get the smiley faces. I would love to see a message like YAY with like a police sticker, I don't know, and your name. You protected your colleagues, or you protected the organization from such and such, and the consequences could have been this." [U21]*

End-of-year recognition was suggested by a few participants as a way to acknowledge and appreciate the efforts of those who consistently reported phishing incidents throughout the year: *"it can be announced once a year. As in we have, uh awarded. I don't know 500 people because of their reporting this year. And that's done in the annual Christmas* *message from the ICT department. [U1]*" Recognizing the top performers in reporting throughout the year would not only acknowledge their dedication but also motivate others to actively participate. Participants were also enthusiastic about department-wise competitions and believed they could serve as an engaging and educational approach to raise awareness about phishing threats and encourage reporting. A few participants mentioned the potential use of gamification elements within the reporting process, such as badges or achievement milestones, to provide a sense of accomplishment and motivation for users: "*I think gamification is a really good incentive, especially because they're all tech-savvy. So I've seen like these buttons or badges saying you reported 100 emails [U24].*" By adding gamified features, the reporting process can become more interactive and encourage users to stay attentive against phishing attempts. Lastly, a few participants suggested the idea of providing tangible rewards like stickers and badges as incentives for completing training modules.

9.4 Chapter Summary

The aim of this chapter was to explore the factors that influence users' reporting behavior in the context of phishing attacks using the COM-B model. The findings shed light on the various aspects of capability, opportunity, and motivation that shape users' actions in identifying and reporting phishing emails.

Regarding capability, users who reported phishing incidents demonstrated a strong sense of self-efficacy in recognizing and reporting suspicious emails. However, they also expressed concerns about the increasing sophistication of phishing emails, which can make them more challenging to detect. In contrast, users who hadn't reported phishing incidents displayed lower levels of confidence and skill in identifying phishing emails. Some participants admitted falling for phishing simulation emails, which undermined their confidence and ability to distinguish legitimate emails from phishing attempts. Limited exposure to real-life examples further hindered their awareness of the broader consequences of phishing attacks on the organization. Some participants also chose to ignore or delete suspicious emails as they weren't aware of the necessity to report them. Similarly, users highlighted lack of awareness of reporting process to be a barrier. With respect to opportunity, participants highlighted the need for clarity and ease of reporting process. Many users who hadn't reported before mentioned their lack of awareness about the reporting process, while even experienced reporters initially struggled to find the correct email address. Exposure to phishing emails also played a role in reporting behavior, especially for users in specific departments, such as HR and Intellectual Property. Some participants who hadn't reported phishing incidents had limited exposure to real phishing attempts. In terms of motivation, participants who reported phishing incidents were intrinsically motivated and viewed reporting as an extension of their work ethic and commitment to doing the right thing. They also expressed a sense of collective responsibility toward their colleagues and the organization as a whole. Personal experiences or knowing someone who had fallen victim to a cyber attack further influenced participants to report incidents. While users generally found the reporting process efficient, concerns about the potential time and effort required were expressed, particularly on busy days. Participants recognized the shared responsibility of keeping the university safe, although some questioned the effectiveness of reporting and the need for clearer communication and feedback from the organization.

With respect to recommendations on enhancements and infrastructure and support systems, participants highlighted the need for educational programs, particularly during onboarding and the start of the academic year, to raise awareness about phishing attacks. They emphasized clear communication, engaging training sessions, and the use of real-life examples to educate users about phishing tactics and risks. Phishing simulations were recognized as effective tools for improving users' ability to identify and report phishing attempts. While a majority of the participants mentioned the usefulness of up-to-date information on phishing trends, common techniques, and examples of successful attacks, they were not aware of existence of the security and privacy website. Participants mentioned the reporting process could be improved with a dedicated report button within the email client and stressed on the importance of regular reminders and updates on the reporting process. Meaningful feedback was deemed essential, including confirmation of the legitimacy of reported emails and informative guidance on handling similar situations in the future. Participants expressed the desire for personalized responses tailored to their specific concerns, rather than generic automated messages. While incentives were acknowledged as a potential motivator, participants emphasized the importance of maintaining a reporting culture centered around protecting the organization. Suggestions for incentives included personalized acknowledgments with visual elements, end-of-year recognition for consistent reporting, department-wise competitions, and gamification features such as badges.

10 Discussion

The discussion chapter aims to comprehensively analyze and interpret the findings obtained from the research on fostering a reporting culture to combat phishing attacks. Employing a mixed-method approach that considers organizational and human factors, the study sought to understand the complexities involved in promoting reporting behavior within the organization.

10.1 Results Discussion

To address SRQ1: "What measures and processes are currently in place within the organization to prevent phishing attacks?", interviews were conducted with the ICT team and security solution providers. The findings revealed that the organization follows a multi-layered approach by partnering with different companies that provide a range of solutions. This approach aligns with the recommendations of Rendall et al. (2020), who emphasize the importance of adopting a multi-layered approach in combating phishing attacks (Rendall et al., 2020). Such an approach involves implementing various security measures and strategies across different levels of an organization's infrastructure. Additionally, the effectiveness of the technical solutions was supported by user interviews, where the majority of participants mentioned not receiving phishing emails except during the phishing simulation exercises. However, the analysis of reported phishing emails in Chapter 8 highlighted the need for further optimization of technical filters, as some phishing emails that were clearly identifiable managed to bypass the filters. Another insight from the security team interviews was the utilization of more sophisticated email filters for faculty and support staff. This decision was driven by their access to corporate-sensitive data, aiming to mitigate the potential risk to the organization in the event of successful phishing attacks on these user groups. While students may not have direct access to corporate-sensitive data, it is crucial to recognize that they are still exposed to various types of risks. During the user interviews, Participant U19 highlighted an account of their friend falling victim to a phishing attack through a spoofed university account in another institution. This raises important questions about the vulnerability and risk exposure of students to phishing attacks. While the burden of the financial impact may not directly fall on the organization, it is important for the organization to take steps to protect all user groups from the potential risks and consequences of phishing attacks. It's vital to acknowledge that the impact on user groups should be considered beyond the protection of sensitive data alone. Different user groups may face distinct risks and consequences in the event of a successful phishing attack, necessitating a comprehensive approach to security measures that safeguard all stakeholders involved. Moreover, it is crucial to recognize the distinction between individual risk and organizational risk in the context of phishing attacks. While the organization may possess more extensive resources to manage potential consequences, individual users may have limited means to cope with impact of successful attacks. Hence the organization should implement technical measures that account for the potential impact on both the organization and individual users, ensuring a well-rounded security strategy.

Apart from the technical measures, the organization recognizes that protecting itself from phishing attacks requires a collaborative effort and views the users as an integral part of the solution. It aligns with the shifting cybersecurity mindset that emphasizes the role of humans as a solution rather than a problem (Zimmermann & Renaud, 2019). In line with this perspective, the organization implements various educational initiatives, with phishing simulations being the most prominent method. The security team believes that embedded training, which involves providing simulated phishing emails to individuals without prior notification, is an effective approach. This aligns with the findings of Siadati (2017), who suggests that embedded training can be more effective than traditional non-embedded training because it simulates real-life scenarios and allows users to learn from their mistakes (Siadati, 2017). The findings of this research indicate that the organization's phishing simulation emails effectively emulate the persuasion techniques employed in real-life phishing attacks. The majority of participants in the study also found phishing simulations to be effective. However, the analysis of user engagement with the training material on the landing page, which users are redirected to after clicking on a phishing simulation link, revealed limited engagement. This finding is consistent with research by Caputo et al. (2014), which suggests that while embedded training provides valuable teaching opportunities, immediate feedback and tailored framing alone may not be sufficient to achieve the desired outcomes of reducing click rates or increasing reporting (Caputo et al., 2014).

During interviews with the ICT team, the importance of reporting phishing incidents emerged as a recurring theme. The security team emphasized the promptness of reports, valuing speed over quantity, as a crucial feedback mechanism for assessing the effectiveness of technical solutions and enabling early detection and prevention. However, this shift in responsibility from infrastructure to users comes with its own costs and challenges. Users are required to invest additional time and effort in the reporting process, diverting their attention from primary tasks and potentially impacting productivity. Herley (2009) emphasizes that users' rejection of security advice is rational from an economic standpoint, as it often imposes indirect costs or externalities (Herley, 2009). Therefore, organizations must recognize and acknowledge the effort and costs borne by users in the reporting process. Moreover, the expectation of prompt reporting places significant pressure on users, potentially pushing them beyond their compliance threshold (Beautement et al., 2008). Users may feel overwhelmed by the added responsibility of consistently monitoring their emails for potential phishing threats. This raises questions about the long-term sustainability of the reporting culture and its potential impact on users productivity (Lain, Kostiainen, & Čapkun, 2022). To ensure users active contribution to the organization's security efforts, it is essential for organizations to prioritize communication and transparency while also taking steps to ensure the reporting process is efficient. By effectively communicating the purpose and significance of user training and phishing simulation exercises, users can understand their crucial role as the organization's first line of defense and the shared responsibility for cybersecurity (Zimmermann & Renaud, 2019). This empowers users to actively participate in reporting and other security measures, contributing to the overall security posture of the organization. Striking a balance between fostering a reporting culture and considering individual compliance thresholds will be crucial in maintaining users' active involvement and commitment to security.

To address *SRQ2: "What is the current state of clicking and reporting behavior among individuals who have received phishing simulation emails?"*, the phishing simulation logs were analyzed. The click rates of the second round of phishing simulations conducted in the organization were observed to be 26.1%, which may appear high at first glance. However, it is essential to consider that click rates can vary depending on the contextual relevance of the phishing email. Research by Steves et al.(2020) indicates that highly contextually relevant phishing emails can lead to significant spikes in click rates (Steves et al., 2020). Participants in the study highlighted that the simulation emails were difficult to detect as they closely resembled genuine organization communications. In evaluating the effectiveness of the phishing simulations, the organization tracks various metrics, including the number of emails sent, clicked, and reported. While the reporting rate of 6.1% may seem low, it is important to note that 2610 unique reports were generated. In the context of a real phishing attack, this number would be considered significant, as even a single report can trigger appropriate action by the security team. However, in the context of phishing simulations, the organization places importance on a higher reporting rate. This helps gauge user awareness and serves as a means to educate users about the necessary actions in case they encounter a suspicious email. From the organization's perspective, while one report is sufficient for action, they recognize the absence of a hive mindset among users. They prefer multiple individuals reporting rather than assuming someone else has already done so. Although the organization does not have a specific target reporting rate in mind, they aim to encourage as many users as possible to report suspicious emails. Reporting, however, comes with costs for the organization in terms of lost labour productivity and the opportunity cost for students. Users need to treat every email with caution, investing additional time and effort to carefully scan and evaluate the presence of phishing cues and red flags. Based on user interviews, it was evident that many users were not aware of the reporting process, leading to a one-time cost of either seeking clarification from colleagues/peers or visiting the website for guidance. Additionally, with phishing simulation campaigns occurring four times a year, users are required to dedicate time and effort to report emails during these simulations. These costs impact productivity as users are not compensated for the time and effort invested in reporting. The shift in focus from primary tasks to reporting and the additional cognitive load imposed on users can potentially hinder their overall productivity. Herley (2009) highlights the challenge of balancing the benefits (reduction of direct losses) and costs (increase in effort) of security advice, emphasizing the need to consider aggregate estimates across the entire user population (Herley, 2009).

The cost-benefit tradeoff of fostering a reporting culture within the organization is a critical consideration. Calculations were conducted to estimate the cost of lost labor productivity for the organization and the opportunity cost for students in an academic year (200 days). Detailed breakdowns of these calculations can be found in the Appendix A.4 and A.5. Based on user interviews, it was found that faculty and support staff receive an average of 15 emails per day, while students receive around 7 emails per day. It was assumed that users spend approximately 5 seconds on preprocessing and scanning for cues or red flags in each email. Additionally, it was estimated that 50% of users were unaware of the reporting procedure, resulting in a one-time cost of 120 seconds to seek clarity on the process. The time required to report an email was estimated at 5 seconds, and users are expected to report at least 4 emails per academic year based on the number of phishing simulations conducted. For faculty and support staff, the calculation considered the average salary (EUR 46K/year @ 28.75 EUR/hour) (Payscale, 2023). Assuming 100% reporting, the loss of labor productivity amounted to 56,407.58 hours, with a corresponding cost of EUR 1,621,717 (56,407.58 hours * 28.73 EUR/hour) per academic year. For students, the calculation accounted for the opportunity cost of tuition fees, considering 10% as international students (EUR 15K/year @ EUR 9.38/hour) and 90% as EU/EFA students (EUR 2,500/year @ EUR 1.56/hour). Assuming 100% reporting, the lost opportunity cost for students amounts to 56,936.97 hours, with a corresponding cost of EUR 133,446.02 (56,936.97 hours * (10% * 9.38 EUR/hour + 90% * 1.56 EUR/hour)). Despite the conservative nature of these figures, the cost to the organization and the users remains substantial.

On the other hand, it is important to assess the potential benefits of maintaining a strong reporting culture. As the organization hasn't suffered any data breaches in the recent past, previous incidents were taken as a reference to highlight the significant financial costs associated with attacks on educational institutions. For example, Maastricht University made a payment of EUR 200,000 as a result of a ransomware attack (Bannister, 2020). Furthermore, US universities have reported a range of costs from EUR 250,000 to EUR 850,000 for similar incidents (Bischoff, 2022). These numbers shed light on the potential financial impact that successful phishing attacks can have on educational institutes. To ensure that the benefits of a reporting culture outweigh the associated costs, the organization should carefully consider the intended outcome or desired level of user reporting. This raises interesting questions about determining the threshold at which users are adequately informed and aware of the reporting process. It is crucial to take into account the implications on labor productivity and the potential impact on the core business of the organization. It is interesting to note that at the current reporting rate for faculty and support staff, which stands at 16.1%, the cost to the organization in terms of lost labor productivity amounts to EUR 261,096.58 per academic year. Remarkably, this figure exceeds the ransomware payment made by Maastricht University. However, it is important to note that the financial impact figures might not consider the potential fines that might be imposed as a result of a GDPR breach or reputational damage. The purpose of these calculations is not to imply that the current state of reporting is optimal. Instead, they highlight the need for the organization to take proactive steps in streamlining the reporting process and reducing the time and costs spent by users on reporting. Implementing a dedicated reporting button and raising awareness about reporting procedures throughout the organization can significantly enhance reporting efficiency and cost-effectiveness. Furthermore, when looking at the lost opportunity cost for students, it is crucial for the organization to acknowledge that user effort is not without value and should not treat the user's attention and effort as an unlimited resource. (Herley, 2009). Understanding the actual worth of user time provides valuable insights into the real cost of security measures to both the organization and its users. Striking a balance between promoting a reporting culture and minimizing disruptions to the organization's operations while considering the impact on users becomes imperative in achieving effective risk mitigation and maintaining a productive work environment. While click rates and reporting rates provide valuable insights, it is important to consider other metrics as well. Metrics such as time intervals between receiving and clicking, the time difference between the first click and the first report, number of repeated clickers as suggested by Steves et al. (2020), offer a deeper understanding of user response patterns (Steves et al., 2020). Additionally, evaluating the open rate of phishing simulation emails, which indicates the percentage of users who accessed the email but did not click on malicious links or report the phishing attempt, provides valuable insights into user behavior and engagement (Rizzoni et al., 2022).

The analysis of the time interval between receiving and clicking the link in the phishing simulation emails further emphasizes the criticality of prompt reporting. It was observed that approximately 25% of users who clicked on the phishing email did so within the first hour. This finding highlights the urgency of reporting suspicious emails promptly, as a significant percentage of individuals may interact with phishing emails within a short span of time. Notably, a report by Proofpoint reveals that 52% of phishing victims click on malicious links within one hour (ProofPoint, 2019). Therefore, in the event of an actual phishing attack, a delay in reporting could have dire consequences for the organization. The research also sheds light on the clicking and reporting behavior of different user groups in the organization. The analysis has revealed that students and faculty members emerge as the most vulnerable groups in terms of susceptibility to phishing attacks. This finding highlights the organization should develop targeted awareness and training programs that address the specific needs and vulnerabilities of these user segments (Vishwanath et al., 2018). Additionally, the data highlights the presence of repeated clickers, accounting for approximately 6.28% of users. It is essential to approach repeated clickers with understanding and support rather than punishment. Instead of blaming or penalizing these users, it is crucial to delve into their perspectives and challenges. As suggested by Canham et al. (2021), gaining a deeper understanding of their experiences, organizations can identify the underlying factors contributing to their repeated clicking behavior and develop strategies to bolster their confidence and resilience against phishing attacks (Canham, Posey, Strickland, & Constantino, 2021). This user-centric approach promotes a culture of learning and improvement, fostering a positive environment where users feel supported and empowered in their cybersecurity practices.

To answer *SRQ3: "How does the design of phishing simulation emails compare to the characteristics and techniques of emails that bypass technical filters"*, document analysis of the reported phishing emails was conducted. The findings of this study reveal that the authority and scarcity principles are the most prevalent persuasion techniques observed in reported phishing emails, and these techniques were successfully replicated in the phishing simulation emails conducted by the organization. This aligns with previous research that identifies authority as the most popular persuasion technique and highlights the high involvement of the scarcity principle in targeting administrators and account-related concerns (Akbar, 2014). By incorporating these techniques into the phishing simulations, users were exposed to realistic scenarios that aimed to enhance their skills in identifying and responding to sophisticated phishing attacks. Additionally, the analysis of common days and times for phishing attempts showed that Mondays and Fridays were the most common, which aligns with a report by Egress (2021) that identified Monday, Saturday, and Friday as peak days for phishing activities (Egress, 2023). This information is valuable for raising user awareness and promoting a proactive approach to combat phishing attacks. By identifying these high-risk periods, the organization can encourage users to exercise extra caution and remain vigilant during those times, enhancing their ability to detect and report suspicious emails. Moreover, incorporating the findings of this analysis into awareness programs can provide engaging material that educates employees about the specific risks they may face during their busy work schedules. By highlighting the prevalence of phishing attempts during certain days and times, employees can be better prepared and informed about potential threats. Additionally, closely monitoring the network and system during these identified high-risk periods allows the organization to implement proactive measures and swiftly respond to potential phishing attacks, safeguarding its infrastructure and data.

To address *SRQ4: "What are the main factors that influence an individual's decision to report or not report phishing emails" and SRQ5: "How can infrastructure and support be enhanced to improve an individual's ability to recognize and report phishing attempts?"*, interviews were conducted with different user groups. The study employed the COM-B model of behavior to investigate the factors influencing reporting behavior and also recommendations to enhance infrastructure and support systems. Under the Capability aspect of the COM-B model, it was observed that the self-efficacy of users, or their ability to identify phishing emails accurately, directly impacted their reporting behavior. This finding aligns with the research by Kwak et al. (2020), which demonstrated that users' self-efficacy toward performing anti-phishing behaviors influences reporting (Kwak et al., 2020). Aligning with Distler's (2023) findings, participants mentioned alternative actions to reporting, such as deleting or ignoring the email, but lacked awareness of the importance of reporting to safeguard the organization (Distler, 2023). While these actions align with what is expected in terms of secure behavior, it raises interesting questions on rethinking metrics to judge user awareness. Furthermore, the awareness of the potential consequences of phishing attacks and the understanding of the reporting process were found to impact reporting behavior. Users who were more aware of the potential consequences associated with phishing attacks and had a clear understanding of how to report such incidents were more likely to engage in reporting. These findings suggest that increasing users' awareness of the potential risks and the importance of reporting can contribute to fostering a reporting culture within the organization. Participants in the study expressed the belief that training sessions conducted during the onboarding process or at the start of the academic year would be helpful in raising awareness about phishing threats, and they were more likely to engage with such initiatives. However, they emphasized the importance of making these training sessions interactive and engaging, avoiding the traditional, monotonous slide-based approach. This finding is consistent with the recommendations from Tally et al.(2023), who emphasize the need for enjoyable and interactive training experiences that mimic the media and conversations users voluntarily engage with in their daily lives (Tally et al., 2023). To enhance awareness, participants suggested using real-life cases and constant reminders through various mediums such as posters, university screens, and even coffee machines. These suggestions align with Tally et al.'s (2023) proposal that information distribution should strike a balance between the surprising and the predictable, utilizing attention-grabbing methods to generate curiosity and promote phishing awareness (Tally et al., 2023).

In the opportunity category, the ease of reporting was identified as a crucial factor influencing reporting behavior. Participants in the study expressed enthusiasm about the implementation of a reporting button, believing that such a feature would make the reporting process more efficient. This finding aligns with research by Distler (2013), which emphasized the importance of making reporting procedures as simple as possible to facilitate user engagement in reporting activities (Distler, 2023). Moreover, the implementation of the report button can serve as a cost-saving measure for users allowing them to quickly report potential phishing emails without having to invest excessive time and effort. Additionally, colleagues and social norms play a role in shaping reporting behavior, with individuals being influenced by the reporting behavior of their peers and perceived social norms. This is supported by Marin et al. (2023) which demonstrates the impact of social norms on shaping individuals' security-related behaviors (Marin et al., 2023). Under motivation, the research found that personal work ethic & values and collective responsibility towards protecting colleagues and the organization influenced reporting behavior. Participants expressed that reporting phishing incidents was the right thing to do, reflecting their personal values and a sense of alignment with the organization's expectations. Previous research has shown a positive relationship between cyber security behaviors and the organizational citizenship behavior (OCB) construct (Dreibelbis, 2016). Personal experiences or knowledge of someone who has fallen victim to a cyber attack were found to be influential in motivating participants to report incidents. It is interesting to note that participants also mentioned that the organization should raise awareness about the real-life consequences and share relevant case studies or stories to illustrate the potential impact on individuals and organizations. Lastly, the perceived effectiveness of reporting, including the provision of acknowledgment and feedback, also impacts reporting behavior. Research by Pilavakis et al. (2023) emphasizes the importance of gaining the trust of users by providing customized feedback to encourage reporting (Pilavakis et al., 2023). When individuals receive timely and tailored feedback on their reported incidents, it reinforces their belief that their actions are valuable to the organization's security efforts.

The participants in the study expressed mixed reactions regarding incentives for reporting phishing incidents. While many acknowledged the appeal of incentives, they emphasized that their primary motivation was to protect themselves and the organization. Striking the right balance is critical to ensure that the core responsibilities of the organization are not overshadowed or detracted from. One potential downside of incentives potential challenges associated with incentivized reporting, such as the risk of an increase in false positives. This aligns with Jensen et al.'s (2022) research, which points out that organizations may inadvertently create an unbalanced incentive structure that overly favors reporting hits, potentially compromising the accuracy and validity of reported incidents (Jensen et al., 2022a). However, the research finds that it is worth exploring the potential of acknowledgment, recognition, and gamification elements as effective strategies for fostering a reporting culture within the organization. It is also important to highlight that incentives and gamification measures for reporting phishing incidents do not eliminate the costs borne by users. While they may appear attractive, they can be seen as a way to encourage users to accept and absorb the cost rather than eliminate it. They should be carefully designed to ensure they do not shift users' focus away from their primary tasks and responsibilities and hence striking a balance between encouraging reporting and maintaining productivity is crucial. With this in mind, acknowledgment and credit for reporting can serve as effective motivators, reinforcing employees' sense of responsibility and encouraging their active participation in reporting phishing incidents.

While acknowledging the importance of fostering a reporting culture within the organization to combat phishing attacks, it is equally crucial to recognize and address the associated costs for both users and the organization. To begin with, it is essential to implement a reporting process that isn't time-consuming and eases the burden on the user. This can be achieved by developing user-friendly interfaces, streamlining reporting procedures, and ensuring consistent communication and transparency. Comprehensive support systems and training programs should be provided to educate users on the significance of reporting and their vital role in safeguarding the organization's security. Implementing feedback mechanisms will reinforce the value placed on users' time and effort in reporting incidents. As emphasized by Zimmermann & Renaud (2019), it is vital to view individuals as valuable contributors to the solution rather than perceiving them as the problem in building a reporting culture. This perspective fosters a collaborative environment where users feel empowered to actively participate in reporting incidents (Zimmermann & Renaud, 2019). Additionally, to optimize user efforts and minimize reporting redundancy, the organization should leverage technology. For instance, implementing a notification or banner system for emails that have already been reported as malicious can prevent users from repeatedly reporting the same emails. This not only saves users' time but also emphasizes the importance of reporting while conveying the organization's appreciation for users' commitment. Exploring the possibility of automatically removing flagged emails from users' inboxes can further streamline the reporting process. Looking ahead, the long-term goal in the cybersecurity realm should be to shift the burden of reporting away from individual users. Although a comprehensive solution may not be readily available,Drawing inspiration from examples such as Google's replacement of CAPTCHAs with "Are you a Robot?" and WhatsApp's implementation of end-to-end message encryption, where technological advancements relieved users from certain responsibilities, opens the possibility for future innovations.

10.2 Validity & Reliability

In order to ensure the reliability and validity of the research findings, various measures were taken. Firstly, a systematic approach was followed in the design and execution of the study, ensuring that the research methods employed were appropriate for investigating the research objectives. Multiple data collection methods, including interviews, document analysis, and quantitative logs, were used to triangulate the findings and enhance the validity of the results. To enhance reliability, steps were taken to address potential threats such as participant error, participant bias, researcher error, and researcher bias. The research included interviews with individuals from different roles in the ICT department to gather the Security team's perspective. On the user side, interviews were conducted with students, faculty, and support staff, aiming to gather diverse perspectives on the factors influencing reporting behavior. A comfortable and conducive atmosphere was established during the interviews to address participant bias, encouraging participants to provide honest and authentic responses (Cypress, 2017). Interviews were conducted in a one-on-one setting, ensuring that participants felt at ease and were not influenced by social desirability or the presence of others. To minimize researcher error, consistent interpretation and analysis of the collected data were ensured (Brink, 1993). Interviews were spread out over a 6-week time-period to maintain a fresh perspective and avoid potential fatigue or mental exhaustion that could compromise data interpretation. The accuracy of transcriptions and interpretations was verified through careful review of interview recordings. Furthermore, to minimize researcher bias, the interviews were approached with an open mind, without any preconceived ideas or personal biases. The primary focus was on truly listening to the participants and understanding their perspectives and experiences.

10.3 Limitations of the Study

While this study aimed to explore the factors influencing reporting behavior and how organizations can enhance their infrastructure and support to foster a reporting culture to combat phishing attacks, there are several limitations that should be acknowledged. Firstly, it is important to note that the research was conducted within a single education institute, which may limit the generalizability of the findings to other organizational settings. Each industry and sector may have unique characteristics and organizational cultures that can influence reporting behavior differently. Secondly, the sample size of users in this study was relatively small, which may impact the representativeness of the findings and the ability to detect subtle variations in reporting behavior. While efforts were made to recruit participants from various backgrounds, a larger and more diverse sample would enhance the statistical power and strengthen the external validity of the results. Furthermore, at the time of conducting this study, the last round of the phishing simulation campaign had not been conducted, and data for the third round was still being compiled. As a result, the study's insights were based on available data up to that point, and a more comprehensive analysis of all four rounds would have provided better insights into trends and patterns related to reporting behavior. Additionally, the sample size of reported emails that were analyzed to identify characteristics of phishing emails was relatively limited. A larger sample would have allowed for a more in-depth exploration of phishing email characteristics, providing a more comprehensive understanding of the types of phishing attempts encountered by the organization. Lastly, the study relied on self-reported data, which is subject to response biases and may not always reflect actual behavior. Participants' perceptions, beliefs, and intentions may not perfectly align with their actual reporting behavior in real-world scenarios. Future research could consider incorporating objective measures or behavioral observations to supplement self-reported data.

10.4 Future Research

In terms of future research, there are several additional avenues that can contribute to the understanding of reporting behavior in the context of phishing attacks. First, conducting a survey-based study to validate and further explore the identified factors can enhance the generalizability of the findings. This can involve administering surveys to larger and more diverse sample sizes, including users from different organizations and industries, to assess the prevalence and significance of these factors across various contexts. Furthermore, it is crucial to delve deeper into user groups and explicitly acknowledge the heterogeneity within them, including students, faculty, and support staff. Factors such as gender, age, experience, and seniority can significantly influence reporting behavior within these groups and should be taken into consideration to obtain a more representative view. For instance, when examining reporting behavior among students, it is important to consider the differences between international and local students, as their experiences and exposure to phishing attacks may vary. Similarly, for faculty and support staff, seniority and experience can play a role in shaping their approach to reporting incidents. Analyzing how these demographic variables interact with the identified factors can provide valuable insights into the nuanced nature of reporting behavior within different user groups. Additionally, conducting comparative studies across different industries and organizational settings can uncover variations in reporting behavior and shed light on the influence of factors such as organizational culture, industry norms, and technological infrastructure. Understanding these contextual nuances will enable the development of tailored approaches for fostering reporting behavior in different environments. Lastly, future research can focus on designing and evaluating interventions aimed at promoting reporting culture. This may involve implementing awareness campaigns, targeted training programs, or incentive structures. Researchers can employ rigorous evaluation methods, such as randomized controlled trials or quasi-experimental designs, to measure the effectiveness of these interventions in encouraging reporting behavior and mitigating the impact of phishing attacks.

11 Conclusion

11.1 Research Conclusion

In conclusion, this research highlights the importance of fostering a reporting culture within the organization to effectively combat phishing attacks. While it is crucial for the organization to promote reporting, it is equally vital to recognize and address the costs borne by users. Striking a balance between encouraging reporting and acknowledging the investment of users' time and effort is key to fostering a sustainable reporting culture. The main research question focused on identifying strategies and measures required to develop a robust reporting culture, while the sub-research questions delved into various aspects including the current measures and processes in place, clicking and reporting behavior among individuals exposed to phishing simulation emails, characteristics of phishing simulation emails in comparison to actual phishing attempt, factors influencing reporting decisions, and ways to enhance an organization's infrastructure and support systems to facilitate reporting.

The research sheds light on the multi-layered approach to security that the organization has adopted to protect its users from phishing attempts. As phishing attacks become more sophisticated, the continuous evolution of preventive solutions and filters is crucial to keep pace with the evolving techniques employed by attackers. By investing in and regularly updating these measures, the organization can enhance its ability to detect and prevent phishing attacks. Alongside the implementation of these preventive measures, fostering a reporting culture is equally important to empower employees in identifying and promptly reporting suspicious emails. However, it is important for the organization to strike a balance between effective risk mitigation and costs with respect to reporting both to the user and the organization. The organization should ensure that the benefits of a reporting culture outweigh the associated costs and challenges. This can be achieved by carefully evaluating the desired reporting level, taking into consideration the organization's resources, the potential impact of phishing attacks, and the time and effort required from users to report incidents. Factors influencing reporting behavior in the context of phishing attacks were identified through the study. Participants who recognized the potential risks and understood the impact of phishing attacks were more likely to report incidents. On the other hand, those who lacked awareness of the importance of reporting or were unaware of the reporting process tended to resort to alternatives such as deleting or ignoring suspicious emails, which are secure behaviors that protect the individual from immediate harm. However, these actions can inadvertently leave the organization and other peers at risk. Self-efficacy played a significant role, as users who were confident in their ability to identify and report suspicious emails were more inclined to report. Additionally, the level of exposure to real-life examples of phishing attempts influenced participants' awareness of the broader consequences of such attacks on the organization. Lack of awareness of the reporting process and the importance of reporting acted as barriers to reporting behavior.

Opportunities for reporting, including the ease of the reporting process and timely and efficient response mechanisms, were identified as crucial factors in influencing reporting behavior. Participants emphasized the need for a clear and streamlined reporting process that is easily accessible and user-friendly. The availability of a dedicated report button within the email client and regular reminders and updates on the reporting process were suggested to enhance the opportunity for reporting. Moreover, incorporating the report button serves as a cost-saving measure for users, enabling them to swiftly report potential phishing emails without excessive time and effort investment. Furthermore, the role of social norms and the influence of colleagues in creating a reporting culture were highlighted. Participants who viewed reporting as an extension of their work ethic and felt a collective responsibility toward protecting their colleagues and the organization demonstrated higher motivation to report incidents. Personal experiences, such as previous encounters with phishing attacks or knowing someone who had fallen victim to a cyber attack, also influenced participants to report incidents. Additionally, the perceived effectiveness of reporting was influenced by the organization's acknowledgment, feedback, and prompt actions following the reports. When users trust that the organization takes appropriate steps, it fosters a sense of reliability and encourages active participation in reporting potential threats.

Ultimately, to foster a reporting culture within the organization, a collaborative effort is vital, involving the organization, its users, and technical systems. It is crucial to acknowledge that reporting is an additional responsibility for users, and they may bear the cost and invest their time in this endeavor. Highlighting how users act as the first line of defense and showcasing the benefits of their actions in protecting the organization can further motivate reporting behavior. While encouraging reporting is vital, it is essential for the organization to reassess its end goal and determine at what point reporting efforts are sufficient. Striking the right balance between promoting reporting and considering the potential implications on users' productivity and well-being becomes imperative. To facilitate reporting, the process should be streamlined, efficient, and require minimal steps. Acknowledging and providing timely feedback are critical factors in making users feel appreciated for their reporting efforts. Training programs can play a significant role in raising awareness about the consequences of phishing attacks, providing tips and tricks to identify such attempts, and stressing the importance of reporting suspicious activities. Incentive programs should be thoughtfully designed to encourage reporting without shifting users' focus from their primary responsibilities. Creating a culture with a competitive spirit at the department level, where peers and colleagues look out for each other, can enhance reporting rates. As observed in users who have reported multiple times, reporting can become a habit and an integrated part of their behavior, which should be the ultimate goal. Embracing a shift in paradigm that views humans as part of the solution, rather than the problem, is essential in fostering a reporting culture. In this context, the organization should leverage technology to minimize reporting redundancy and optimize the reporting process. Implementing a notification or banner system for emails that have already been reported as malicious can prevent users from repeatedly reporting the same emails. Such measures can effectively streamline the reporting process and convey the organization's appreciation for users' time and commitment. Additionally, exploring the possibility of automatically removing flagged emails from users' inboxes can further alleviate the reporting burden. By implementing these strategies, the organization can create a proactive and vigilant community, collectively safeguarding the organization against phishing attacks and contributing to a more secure digital environment.

11.2 Recommendations

To enhance the reporting culture within the organization and combat phishing attacks effectively, several key recommendations can be implemented.

- **Acknowledging Costs and Streamlining Efforts:** Acknowledging the costs associated with reporting is crucial for the organization to develop an effective cybersecurity strategy. To address this, measures should be implemented to streamline the reporting process and reduce redundancy. By considering the cost-benefit tradeoff, the organization can optimize reporting efforts while minimizing the burden on users. As Herley (2009) suggests, if the cost of security advice exceeds the harm caused by the attack, the advice provided becomes more harmful than the attack itself (Herley, 2009). In line with this, one recommendation is to introduce a notification or banner system for emails that have already been flagged as malicious. Such a system can effectively prevent users from redundantly reporting the same emails, streamlining the reporting process. The accompanying message should not only highlight the significance of reporting but also convey the organization's sincere appreciation for users' commitment and dedication. By implementing this solution, the organization can reinforce the reporting culture while acknowledging the value of users' time and effort in upholding a secure environment.

- **Establish a user-friendly reporting process:** Implement a dedicated report button within the email client, ensuring easy accessibility for users to report suspicious emails. User interviews revealed that reducing the steps required to report suspicious emails would have a positive impact on reporting behavior. This aligns with the research conducted by Distler (2020), which emphasizes the importance of user-friendly reporting mechanisms to encourage timely and accurate reporting of phishing attempts. Additionally, regular reminders and updates about the reporting process should be provided to increase awareness and engagement among users. It is crucial to provide meaningful feedback to users, including confirming the legitimacy of reported emails and offering informative guidance on handling similar situations. This feedback validates users efforts and enhances their understanding of phishing attempts (Lain, Kostiainen, & Čapkun, 2022).

- **Training Programs:** Users showed a positive attitude towards training sessions, particularly during the onboarding of employees and the start of the academic year. To ensure the effectiveness of the training program, it is recommended to incorporate personalized insights into the phishing training. By tailoring the training content to the specific roles and responsibilities of the different user groups, individuals can gain a deeper understanding of how phishing attacks target their specific areas of work. Users also highlighted a lack of exposure to real-life examples and case studies, and hence simulating real-world scenarios and showcasing the consequences of successful phishing attempts can help develop a deeper understanding of the risks involved. Furthermore, integrating real-life examples, trends, and case studies provides practical insights into evolving phishing tactics, reinforcing the relevance of phishing awareness training. Regular training programs can be extended to cover the reporting process, and feedback mechanisms can inform reporters of the outcomes of their reports (Marin et al., 2023). Lastly, using various communication channels such as posters, flyers, and digital displays near communal areas like coffee machines to reinforce key messages can further raise awareness as highlighted by (Tally et al., 2023). In addition to personalized training sessions and real-life examples, regular reminders are crucial in reinforcing users' knowledge of identifying phishing emails. Research by Reinheimer et. al (2020) emphasizes the significance of periodic reminders, at least once every six months after initial training, to ensure users retain the information and stay vigilant against evolving phishing tactics. These reminders can serve as valuable touchpoints, refreshing users' memory on tips and tricks to identify suspicious emails, thereby bolstering the effectiveness of the training program (Reinheimer et al., 2020).

- **"Phish of the Week" Campaign:** To address users' feedback about limited exposure to real phishing attempts, it is recommended to implement a recurring "Phish of the Week" campaign. This initiative showcases real-world phishing attempts through various channels, providing employees with regular educational opportunities. By familiarizing employees with phishing tactics and red flags, the campaign enhances their ability to recognize and respond to such attacks. It also encourages active participation in reporting suspicious incidents, fostering a collaborative approach to cybersecurity.

- **Employee Incentives and Recognition:** Implement an incentive program to recognize and reward employees who consistently report phishing attempts or actively participate in phishing awareness campaigns. Personalized acknowledgments with visual elements, end-of-year recognition for consistent reporting, department-wise competitions, and gamification features such as badges can serve as effective incentives. The implementation of this program aims to boost employee motivation and foster a positive reporting culture. This recommendation is supported by research conducted by Jensen et. al (2022), however, it is recommended to exercise caution to ensure that the incentive program does not shift the focus away from the primary task of reporting phishing emails (Jensen, Wright, Durcikova, & Karumbaiah, 2022b).

- **Internal Communication Channels:** To maximize the effectiveness of internal communication channels, it is essential to raise awareness about dedicated security and privacy websites among employees. The user interviews highlighted that many users were not aware of the existence of such a website. By utilizing internal communication channels such as newsletters, intranet portals, and the security and privacy website, the organization can provide timely and informative updates on phishing trends, common techniques, and successful attacks. Sharing real success stories of how employee reports have contributed to the organization's security can further emphasize the importance of reporting and motivate others to actively participate in the reporting process.

- **Phishing Simulation Campaign Metrics & Results:** In addition to click rates and reporting rates, it is essential for organizations to consider a range of metrics to gain a comprehensive understanding of user behavior in response to phishing attempts. Metrics such as time intervals between email receipt and clicking, the time difference between the first click and the first report, and the number of repeated clickers, as suggested by Steves et al. (2020), offer valuable insights into user response patterns (Steves et al., 2020). Additionally, it is important to consider the open rate, as it provides valuable information on how many users opened the email without taking any further action, which can help gauge users' awareness and their ability to identify potentially malicious content even if they did not interact with the phishing attempt. The organization should also share statistics of phishing simulation programs organization-wide, including department-wise results, to provide transparency and insight into the effectiveness of the program. This transparent approach fosters healthy competition among departments, encourages continuous improvement, and aligns with the research emphasizing the importance of result-sharing in phishing prevention efforts (Rizzoni et al., 2022). To further incentivize departments, introduce an end-of-year recognition program that awards the department with the fastest reporting rates and lowest click rates. This recognition serves as a powerful motivator for departments to prioritize reporting suspicious emails, exercise caution, and reinforces the significance of their contributions to the organization's cybersecurity goals.

11.3 Relevance to MOT Program

This research addresses a socio-technical problem by exploring the relationship between human decision-making and organizational support systems in the context of cybersecurity. The course Inter- and intra-Organisational Decision Making has provided a solid foundation for understanding the cognitive processes involved in individual decision-making. This knowledge is integral to comprehending the various factors that influence reporting behavior in phishing incidents. As part of the Cybersecurity specialization, the course on user-centered security emphasizes the significance of considering human behavior and decision-making processes when designing effective security measures. It challenges the traditional approach of solely blaming human error for security breaches and highlights the importance of organizational factors. This study explores how the organization can enhance their infrastructure and support systems to empower users and cultivate a reporting culture, thereby mitigating phishing attacks.

References

Abawajy, J. (2012, August). User preference of cyber security awareness delivery methods. *Behaviour Information Technology*, *33*(3), 237–248. Retrieved from https://doi.org/10.1080/0144929x.2012.708787 doi: 10.1080/0144929x.2012.708787

Adams, W. (2015). Conducting semi-structured interviews. In K. E. Newcomer, H. P. Hatry, & J. S. Wholey (Eds.), *Handbook of practical program evaluation* (p. 492-505). Jossey-Bass, a Wiley Imprint.

Akbar, N. (2014, October). *Analysing persuasion principles in phishing emails.* Retrieved from http://essay.utwente.nl/66177/

Akhawe, D., & Felt, A. P. (2013). Alice in warningland: A large-scale field study of browser security warning effectiveness. In *Proceedings of the 22nd usenix conference on security* (p. 257–272). USA: USENIX Association.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*. doi: 10.3389/fcomp.2021.563060

Alnajim, A. M., & Munro, M. (2009). An approach to the implementation of the anti-phishing tool for phishing websites detection. *2009 International Conference on Intelligent Networking and Collaborative Systems*, 105-112.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M., Levi, M., ... Savage, S. (2012, 01). Measuring the cost of cybercrime..

APWG. (2022). *3rd quarter 2022 - docs.apwg.org.* Anti-Phishing Working Group. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf

Bahnsen, A. C., Torroledo, I., Camacho, L. D., & Villegas, S. (2018). Deepphish : Simulating malicious ai..

Bakarich, K. M., & Baranek, D. (2019). Something phish-y is going on here: A teaching case on business email compromise. *Current Issues in Auditing*, *14*(1). doi: 10.2308/ciia-52706

Bann, L. L., Singh, M. M., & Samsudin, A. (2015). Trusted security policies for tackling advanced persistent threat via spear phishing in byod environment. *Procedia Computer Science*, *72*, 129-136. Retrieved from https://www.sciencedirect.com/science/article/pii/S1877050915035747 (The Third Information Systems International Conference 2015) doi: https://doi.org/10.1016/j.procs.2015.12.113

Bannister, A. (2020, Feb). *Ransomware attack: Maastricht university pays out $220,000 to cybercrooks.* The Daily Swig. Retrieved from https://portswigger.net/daily-swig/ransomware-attack-maastricht-university-pays-out-220-000-to-cybercrooks

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: Analysis and perspectives. *IEEE Access*, *9*, 148353–148373. doi: 10.1109/access.2021.3123894

Beautement, A., Sasse, M. A., & Wonham, M. (2008, 9). The compliance budget.. Retrieved from https://doi.org/10.1145/1595676.1595684 doi: 10.1145/1595676.1595684

Beuran, K.-i. T. Y. S. Y., Razvan Chinen. (2016). Towards effective cybersecurity education and training.

Bischoff, P. (2022). *Ransomware attacks on US schools and colleges cost $9.45bn in 2022.* Retrieved from https://www.comparitech.com/blog/information-security/school-ransomware-attacks

Brink, H. I. L. (1993). Validity and reliability in qualitative research. *Curationis*, *16*(2), a1396. Retrieved from https://doi.org/10.4102/curationis.v16i2.1396 (This work is licensed under CC Attribution 4.0) doi: https://doi.org/10.4102/curationis.v16i2.1396

Burda, P., Allodi, L., & Zannone, N. (2021, September). Dissecting social engineering attacks through the lenses of cognition. In *Proceedings - 2021 ieee european symposium on security and privacy workshops, euro s and pw 2021* (pp. 149–160). doi: 10.1109/EuroSPW54576.2021.00024

Canham, M., Posey, C., Strickland, D., & Constantino, M. J. (2021, 1). Phishing for Long Tails: Examining Organizational Repeat Clickers and Protective Stewards. *SAGE Open*, *11*(1), 215824402199065. Retrieved from https://doi.org/10.1177/2158244021990656 doi: 10.1177/2158244021990656

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, *12*, 28-38.

Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of security awareness training on phishing click-through rates. *2017 IEEE International Conference on Big Data (Big Data)*, 4458-4466.

Chowdhury, N., & Gkioulos, V. (2021, 05). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361. doi: 10.1016/j.cosrev.2021.100361

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches.* Sage Publications.

Cui, Q., Jourdan, G.-V., Bochmann, G. V., Couturier, R., & Onut, I.-V. (2017). Tracking phishing attacks over time. *Proceedings of the 26th International Conference on World Wide Web*. doi: 10.1145/3038912.3052654

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research. *Dimensions of Critical Care Nursing*, *36*(4), 253–263. Retrieved from https://doi.org/10.1097/dcc.0000000000000253 (Retrieved from https://doi.org/10.1097/dcc.0000000000000253) doi: 10.1097/dcc.0000000000000253

Dearnley, C. (2005, 1). A reflection on the use of semi-structured interviews. *Nurse Researcher*, *13*(1), 19–28. Retrieved from https://doi.org/10.7748/nr2005.07.13.1.19.c5997 doi: 10.7748/nr2005.07.13.1.19.c5997

Distler, V. (2023). The influence of context on response to spear-phishing attacks: An in-situ deception study. In *Proceedings of the 2023 chi conference on human factors in computing systems.* New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/3544548.3581170 doi: 10.1145/3544548.3581170

Dreibelbis, R. C. (2016). *It's more than just changing your password: Exploring the nature and antecedents of cyber-security behaviors* (Graduate Theses and Dissertations). USF Tampa.

Egelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the sigchi conference on human factors in computing systems* (p. 1065–1074). New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/1357054.1357219 doi: 10.1145/1357054.1357219

Egress. (2023). *Email threats pulse report.* Retrieved from https://pages.egress.com/Whitepaper-PulseReport-05-23_2023-Landing-PAGE.html#download

Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human-Computer Studies*, *125*, 19–31. doi: 10.1016/j.ijhcs.2018.12.004

Fette, I., Sadeh, N., & Tomasic, A. (2007). Learning to detect phishing emails. *Proceedings of the 16th international conference on World Wide Web*. doi: 10.1145/1242572.1242660

Fiore, S. M., Caulkins, B., Reinerman-Jones, L., & Canham, M. (2019, 8). The Enduring Mystery of the Repeat Clickers. *ResearchGate*. Retrieved from https://www.researchgate.net/publication/335950167_The_Enduring_Mystery_of_the_Repeat_Clickers

Flick, U., von Kardorff, E., & Steinke, I. (2004). *A companion to qualitative research.*

Greene, K., Steves, M. P., & Theofanos, M. F. (2018, 6). No Phishing beyond This Point. *IEEE Computer*, *51*(6), 86–89. Retrieved from https://doi.org/10.1109/mc.2018.2701632 doi: 10.1109/mc.2018.2701632

Guest, G., Bunce, A., & Johnson, L. (2006, 2). How Many Interviews Are Enough? *Field Methods*, *18*(1), 59–82. Retrieved from https://doi.org/10.1177/1525822x05279903 doi: 10.1177/1525822x05279903

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2016). Fighting against phishing attacks: State of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629–3654. doi: 10.1007/s00521-016-2275-y

Halevi, T., Memon, N., & Nov, O. (2015, 01). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *SSRN Electronic Journal*. doi: 10.2139/ssrn.2544742

Herley, C. (2009, 1). So long, and no thanks for the externalities.. Retrieved from https://doi.org/10.1145/1719030.1719050 doi: 10.1145/1719030.1719050

Hodkinson, P., & Hodkinson, H. (2001). The strengths and limitations of case study research. In *Learning and skills development agency conference at cambridge* (Vol. 1, pp. 5–7).

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74–81. doi: 10.1145/2063176.2063197

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

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020, 1). Why Employees (Still) Click on Phishing Links: An Investigation in Hospitals. *Journal of Medical Internet Research*, *22*(1), e16775. Retrieved from https://doi.org/10.2196/16775 doi: 10.2196/16775

Jansen, J., & Van Schaik, P. (2018, 7). Persuading end users to act cautiously online: a fear appeals study on phishing. *Information computer security*, *26*(3), 264–276. Retrieved from https://doi.org/10.1108/ics-03-2018-0038 doi: 10.1108/ics-03-2018-0038

Jensen, M. L., Wright, R. T., Durcikova, A., & Karumbaiah, S. (2022a). Improving phishing reporting using security gamification. *Journal of Management Information Systems*, *39*(3), 793-823. Retrieved from https://doi.org/10.1080/07421222.2022.2096551 doi: 10.1080/07421222.2022.2096551

Jensen, M. L., Wright, R. T., Durcikova, A., & Karumbaiah, S. (2022b). Improving phishing reporting using security gamification. *Journal of Management Information Systems*, *39*(3), 793-823. doi: 10.1080/07421222.2022.2096551

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007, 4). Toward a Definition of Mixed Methods Research. *Journal of Mixed Methods Research*, *1*(2), 112–133. Retrieved from https://doi.org/10.1177/1558689806298224 doi: 10.1177/1558689806298224

Karumbaiah, S., Wright, R. T., Durcikova, A., & Jensen, M. L. (2016). Phishing training: A preliminary look at the effects of different types of training..

Kersten, L., Burda, P., Allodi, L., & Zannone, N. (2022). Investigating the effect of phishing believability on phishing reporting. *2022 IEEE European Symposium on Security and Privacy Workshops*. doi: 10.1109/eurospw55150.2022.00018

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. I. (2008). Lessons from a real world evaluation of anti-phishing training. *2008 eCrime Researchers Summit*, 1-12.

Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear phishing emails? *Telematics and Informatics*, *48*, 101343. doi: 10.1016/j.tele.2020.101343

Lain, D., Kostiainen, K., & Čapkun, S. (2022). Phishing in organizations: Findings from a large-scale and long-term study. In *2022 ieee symposium on security and privacy (sp)* (pp. 842–859).

Lain, D., Kostiainen, K., & Čapkun, S. (2022). Phishing in organizations: Findings from a large-scale and long-term study. In *2022 ieee symposium on security and privacy (sp)* (p. 842-859). doi: 10.1109/SP46214.2022.9833766

Marforio, C., Masti, R. J., Soriente, C., Kostiainen, K., & Capkun, S. (2016). Hardened setup of personalized security indicators to counter phishing attacks in mobile banking. *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices*. doi: 10.1145/2994459.2994462

Marin, I. A., Burda, P., Zannone, N., & Allodi, L. (2023, 4). The Influence of Human Factors on the Intention to Report Phishing Emails.. Retrieved from https://doi.org/10.1145/3544548.3580985 doi: 10.1145/3544548.3580985

Masood, R., Sirshar, M., & Zainab, Q. (2015, Mar.). Research analysis of cyber security. *Global Journal of Computer Science and Technology*, *15*(E4), 7–10. Retrieved from https://computerresearch.org/index.php/computer/article/view/1209

Menard, P., Bott, G. J., & Crossler, R. E. (2017, 10). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems*, *34*(4), 1203–1230. Retrieved from https://doi.org/10.1080/07421222.2017.1394083 doi: 10.1080/07421222.2017.1394083

Michie, S., van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science : IS*, *6*, 42. doi: 10.1186/1748-5908-6-42

Michie, S., Van Stralen, M. M., & West, R. (2011, 4). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*, *6*(1). Retrieved from https://doi.org/10.1186/1748-5908-6-42 doi: 10.1186/1748-5908-6-42

Nakashima, E., & Harris, S. (2018, Jul). *How the russians hacked the dnc and passed its emails to wikileaks.* WP Company. Retrieved from https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html

Oreilly, L. (2023, Jan). *State of phishing report reveals more than 255 million attacks in 2022.* Retrieved from https://www.slashnext.com/blog/state-of-phishing-report-reveals-more-than-255-million-attacks-in-2022/

Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud amp; Security*, *2012*(1), 8–11. doi: 10.1016/s1361-3723(12)70007-6

Parsons, K., Butavicius, M. A., Pattinson, M. R., Calic, D., McCormac, A., & Jerram, C. (2016). Do users focus on the correct cues to differentiate between phishing and genuine emails? *CoRR*, *abs/1605.04717*. Retrieved from http://arxiv.org/abs/1605.04717

Parsons, K., McCormac, A., Pattinson, M. R., Butavicius, M. A., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Comput. Secur.*, *52*, 194-206.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management Computer Security*, *20*(1), 18-28. Retrieved from https://www.proquest.com/scholarly-journals/why-do-some-people-manage-phishing-e-mails-better/docview/928743574/se-2 (Copyright - Copyright Emerald Group Publishing Limited 2012; Last updated - 2022-11-13)

Payscale. (2023). *Average Salary in College/University Netherlands in 2023 | PayScale.* Retrieved from https://www.payscale.com/research/NL/Industry=College_or_University/Salary

Pilavakis, N., Jenkins, A., Kokciyan, N., & Vaniea, K. (2023). "i didn't click": What users say when reporting phishing. In *Proceedings 2023 symposium on usable security and privacy (usec)* (p. 1-13). The Internet Society. Retrieved from https://doi.org/10.14722/usec.2023.233129 doi: 10.14722/usec.2023.233129

ProofPoint. (2019, 1). *Threat actors follow the money: Proofpoint releases the Human Factor 2018 Report | Proofpoint US.* Retrieved from https://www.proofpoint.com/us/threat-insight/post/threat-actors-follow-money-proofpoint-releases-human-factor-2018-report

Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., ... Volkamer, M. (2020). An investigation of phishing awareness and education over time: When and how to best remind users. , 259–284.

Rendall, K., Nisioti, A., & Mylonas, A. (2020, 8). Towards a Multi-Layered Phishing Detection. *Sensors*, *20*(16), 4540. Retrieved from https://doi.org/10.3390/s20164540 doi: 10.3390/s20164540

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022, 1). Phishing simulation exercise in a large hospital: A case study. *Digital health*, *8*, 205520762210817. Retrieved from https://doi.org/10.1177/20552076221081716 doi: 10.1177/20552076221081716

Rocha Flores, W., Holm, H., Svensson, G., & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management amp; Computer Security*, *22*(4), 393–406. doi: 10.1108/imcs-11-2013-0083

Roman, J., & Ross, R. (2014, Oct). *Chase breach affects 76 million households.* Retrieved from https://www.bankinfosecurity.com/chase-breach-affects-76-million-households-a-7395

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2020, 10). Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter? *Journal of Computer Information Systems*, *61*(6), 539–550. Retrieved from https://doi.org/10.1080/08874417.2020.1812134 doi: 10.1080/08874417.2020.1812134

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). 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.* New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/1753326.1753383 doi: 10.1145/1753326.1753383

Siadati, H. (2017). *Measuring the Effectiveness of Embedded Phishing Exercises.* Retrieved from https://www.usenix.org/conference/cset17/workshop-program/presentation/siadatii

Sirigineedi, S. S., Soni, J., & Upadhyay, H. (2020). Learning-based models to detect runtime phishing activities using urls. *Proceedings of the 2020 the 4th International Conference on Compute and Data Analysis*. doi: 10.1145/3388142.3388170

Stanton, B. C., Theofanos, M. F., Prettyman, S. S., & Furman, S. M. (2016). Security fatigue. *IT Professional*, *18*, 26-32.

Stembert, N., Padmos, A., Bargh, M. S., Choenni, S., & Jansen, F. (2015). A study of preventing email (spear) phishing by enabling human intelligence. *2015 European Intelligence and Security Informatics Conference*. doi: 10.1109/eisic.2015.38

Steves, M., Greene, K., & Theofanos, M. (2020). Categorizing human phishing difficulty: A phish scale. *Journal of Cybersecurity*, *6*(1). doi: 10.1093/cybsec/tyaa009

Tally, A. C., Abbott, J., Bochner, A., Das, S., & Nippert-Eng, C. (2023, 4). Tips, Tricks, and Training: Supporting Anti-Phishing Awareness among Mid-Career Office Workers Based on Employees' Current Practices.. Retrieved from https://doi.org/10.1145/3544548.3580650 doi: 10.1145/3544548.3580650

Van Der Kleij, R., Van 't Hoff-De Goede, S., Van De Weijer, S., & Leukfeldt, R. (2021). *How Safely Do We Behave Online? An Explanatory Study into the Cybersecurity Behaviors of Dutch Citizens.* Retrieved from https://doi.org/10.1007/978-3-030-79997-7_30 doi: 10.1007/978-3-030-79997-7\{_}30

Van Der Kleij, R., Wijn, R., & Hof, T. (2020, 10). An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations. *Computers Security*, *97*, 101970. Retrieved from https://doi.org/10.1016/j.cose.2020.101970 doi: 10.1016/j.cose.2020.101970

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, *45*, 1146 - 1166.

Vishwanath, A., Herath, T. C., Chen, R., Wang, J., & Rao, H. R. (2011, 6). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576–586. Retrieved from `https://doi.org/10.1016/j.dss.2011.03.002` doi: 10.1016/j.dss.2011.03.002

Vrbančič, G., Fister, I., & Podgorelec, V. (2018). Swarm intelligence approaches for parameter setting of deep learning neural network. *Proceedings of the 8th International Conference on Web Intelligence, Mining and Semantics*. doi: 10.1145/3227609.3227655

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security.* Cengage.

Williams, E. J., & Polage, D. (2018). How persuasive is phishing email? the role of authentic design, influence and current events in email judgements. *Behaviour amp; Information Technology*, *38*(2), 184–197. doi: 10.1080/0144929x.2018.1519599

Yin, R. K. (2012). *Case study methods.* Retrieved from `https://doi.org/10.1037/13620-009` doi: 10.1037/13620-009

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, *19*(3), 321–332.

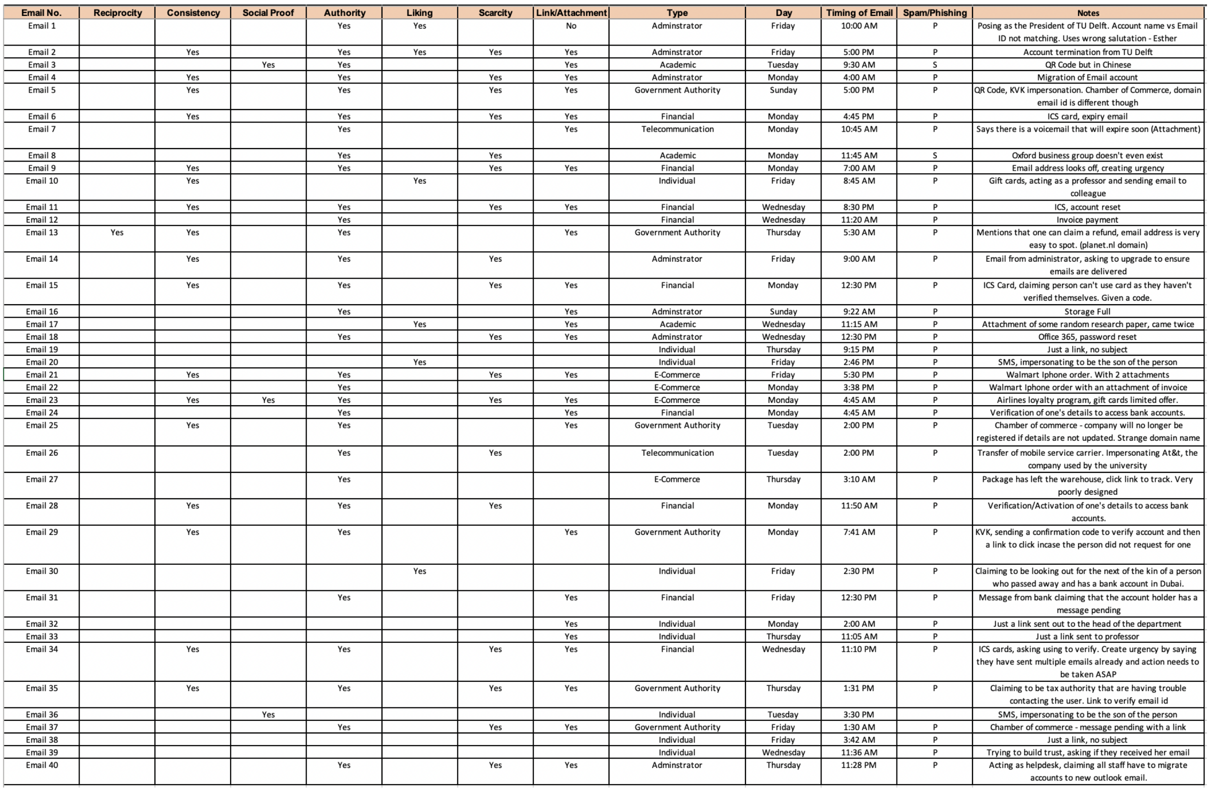
Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, *23*(4), 407-416.

Zimmermann, V., & Renaud, K. (2019, 11). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International journal of human-computer studies*, *131*, 169–187. Retrieved from `https://doi.org/10.1016/j.ijhcs.2019.05.005` doi: 10.1016/j.ijhcs.2019.05.005

Zscaler. (2023). *Zscaler ThreatLabz 2023 Phishing Report* (Tech. Rep.). Retrieved from `https://www.zscaler.com/resources/industry-reports/2023-threatlabz-phishing-report.pdf`

A Appendix

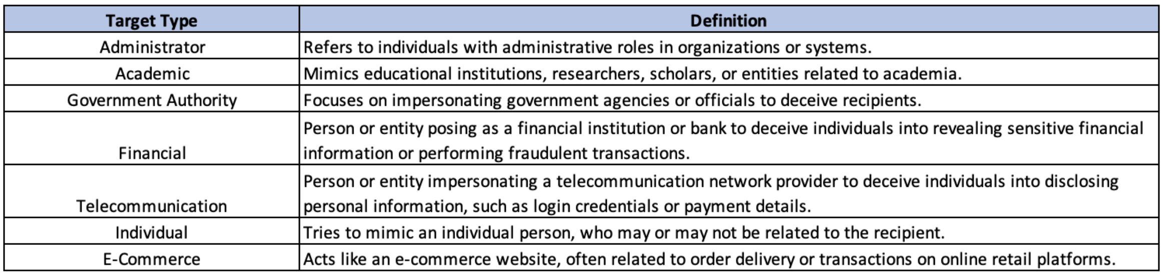
A.1 Reported Phishing Email Analysis



Email No.	Reciprocity	Consistency	Social Proof	Authority	Liking	Scarcity	Link/Attachment	Type	Day	Timing of Email	Spam/Phishing	Notes
Email 1				Yes	Yes		No	Adminstrator	Friday	10:00 AM	P	Posing as the President of TU Delft. Account name vs Email ID not matching. Uses wrong salutation - Esther
Email 2		Yes		Yes	Yes	Yes	Yes	Adminstrator	Friday	5:00 PM	P	Account termination from TU Delft
Email 3			Yes	Yes			Yes	Academic	Tuesday	9:30 AM	S	QR Code but in Chinese
Email 4		Yes		Yes		Yes	Yes	Adminstrator	Monday	4:00 AM	P	Migration of Email account
Email 5		Yes		Yes		Yes	Yes	Government Authority	Sunday	5:00 PM	P	QR Code, KVK impersonation. Chamber of Commerce, domain email id is different though
Email 6		Yes		Yes		Yes	Yes	Financial	Monday	4:45 PM	P	ICS card, expiry email
Email 7				Yes			Yes	Telecommunication	Monday	10:45 AM	P	Says there is a voicemail that will expire soon (Attachment)
Email 8				Yes		Yes		Academic	Monday	11:45 AM	S	Oxford business group doesn't even exist
Email 9		Yes		Yes		Yes	Yes	Financial	Monday	7:00 AM	P	Email address looks off, creating urgency
Email 10		Yes			Yes			Individual	Friday	8:45 AM	P	Gift cards, acting as a professor and sending email to colleague
Email 11		Yes		Yes		Yes	Yes	Financial	Wednesday	8:30 PM	P	ICS, account reset
Email 12				Yes				Financial	Wednesday	11:20 AM	P	Invoice payment
Email 13	Yes	Yes		Yes			Yes	Government Authority	Thursday	5:30 AM	P	Mentions that one can claim a refund, email address is very easy to spot. (planet.nl domain)
Email 14		Yes		Yes		Yes		Adminstrator	Friday	9:00 AM	P	Email from administrator, asking to upgrade to ensure emails are delivered
Email 15		Yes		Yes		Yes	Yes	Financial	Monday	12:30 PM	P	ICS Card, claiming person can't use card as they haven't verified themselves. Given a code.
Email 16				Yes			Yes	Adminstrator	Sunday	9:22 AM	P	Storage Full
Email 17					Yes		Yes	Academic	Wednesday	11:15 AM	P	Attachment of some random research paper, came twice
Email 18				Yes		Yes	Yes	Adminstrator	Wednesday	12:30 PM	P	Office 365, password reset
Email 19								Individual	Thursday	9:15 PM	P	Just a link, no subject
Email 20					Yes			Individual	Friday	2:46 PM	P	SMS, impersonating to be the son of the person
Email 21		Yes		Yes		Yes	Yes	E-Commerce	Friday	5:30 PM	P	Walmart Iphone order. With 2 attachments
Email 22				Yes				E-Commerce	Monday	3:38 PM	P	Walmart Iphone order with an attachment of invoice
Email 23		Yes	Yes	Yes		Yes	Yes	E-Commerce	Monday	4:45 AM	P	Airlines loyalty program, gift cards limited offer.
Email 24				Yes			Yes	Financial	Monday	4:45 AM	P	Verification of one's details to access bank accounts.
Email 25		Yes		Yes			Yes	Government Authority	Tuesday	2:00 PM	P	Chamber of commerce - company will no longer be registered if details are not updated. Strange domain name
Email 26				Yes		Yes		Telecommunication	Tuesday	2:00 PM	P	Transfer of mobile service carrier. Impersonating At&t, the company used by the university
Email 27				Yes				E-Commerce	Thursday	3:10 AM	P	Package has left the warehouse, click link to track. Very poorly designed
Email 28		Yes		Yes		Yes		Financial	Monday	11:50 AM	P	Verification/Activation of one's details to access bank accounts.
Email 29		Yes		Yes			Yes	Government Authority	Monday	7:41 AM	P	KVK, sending a confirmation code to verify account and then a link to click incase the person did not request for one
Email 30					Yes			Individual	Friday	2:30 PM	P	Claiming to be looking out for the next of the kin of a person who passed away and has a bank account in Dubai.
Email 31				Yes			Yes	Financial	Friday	12:30 PM	P	Message from bank claiming that the account holder has a message pending
Email 32							Yes	Individual	Monday	2:00 AM	P	Just a link sent out to the head of the department
Email 33							Yes	Individual	Thursday	11:05 AM	P	Just a link sent to professor
Email 34		Yes		Yes		Yes	Yes	Financial	Wednesday	11:10 PM	P	ICS cards, asking using to verify. Create urgency by saying they have sent multiple emails already and action needs to be taken ASAP
Email 35		Yes		Yes		Yes	Yes	Government Authority	Thursday	1:31 PM	P	Claiming to be tax authority that are having trouble contacting the user. Link to verify email id
Email 36			Yes					Individual	Tuesday	3:30 PM		SMS, impersonating to be the son of the person
Email 37				Yes		Yes	Yes	Government Authority	Friday	1:30 AM	P	Chamber of commerce - message pending with a link
Email 38								Individual	Friday	3:42 AM	P	Just a link, no subject
Email 39								Individual	Wednesday	11:36 AM	P	Trying to build trust, asking if they received her email
Email 40				Yes		Yes	Yes	Adminstrator	Thursday	11:28 PM	P	Acting as helpdesk, claiming all staff have to migrate accounts to new outlook email.

Figure 14: Analysis of Reported Phishing Emails

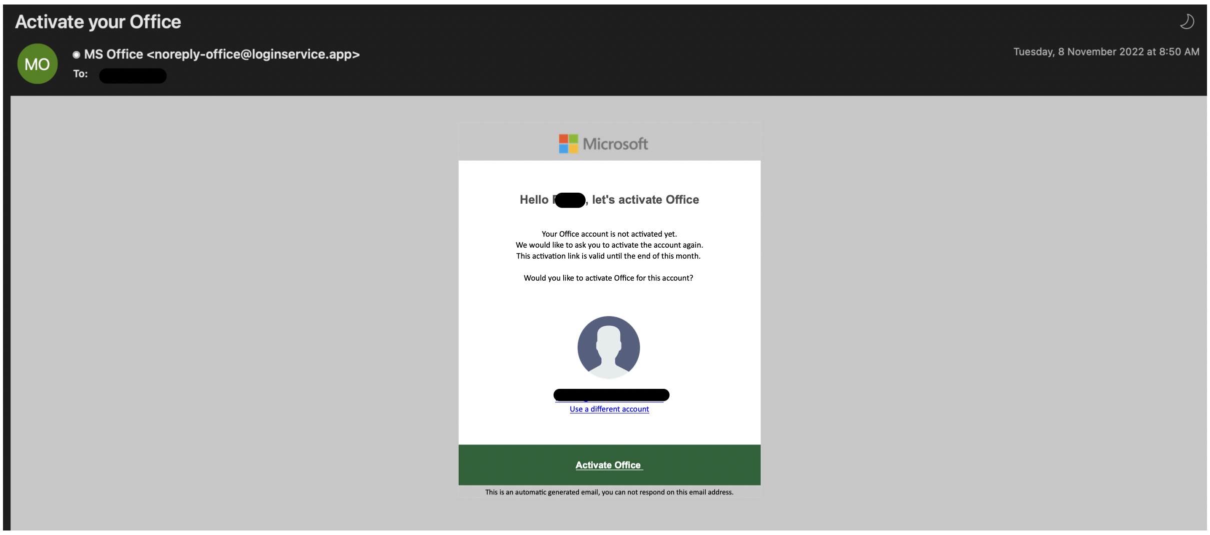
A.2 Target Types



Target Type	Definition
Administrator	Refers to individuals with administrative roles in organizations or systems.
Academic	Mimics educational institutions, researchers, scholars, or entities related to academia.
Government Authority	Focuses on impersonating government agencies or officials to deceive recipients.
Financial	Person or entity posing as a financial institution or bank to deceive individuals into revealing sensitive financial information or performing fraudulent transactions.
Telecommunication	Person or entity impersonating a telecommunication network provider to deceive individuals into disclosing personal information, such as login credentials or payment details.
Individual	Tries to mimic an individual person, who may or may not be related to the recipient.
E-Commerce	Acts like an e-commerce website, often related to order delivery or transactions on online retail platforms.

Figure 15: Types of Targets in Phishing Attempts and their Definitions

A.3 Phishing Simulation Emails



Activate your Office

MS Office <noreply-office@loginservice.app>

To: [redacted]

Tuesday, 8 November 2022 at 8:50 AM

Microsoft

Hello [redacted], let's activate Office

Your Office account is not activated yet.
We would like to ask you to activate the account again.
This activation link is valid until the end of this month.

Would you like to activate Office for this account?

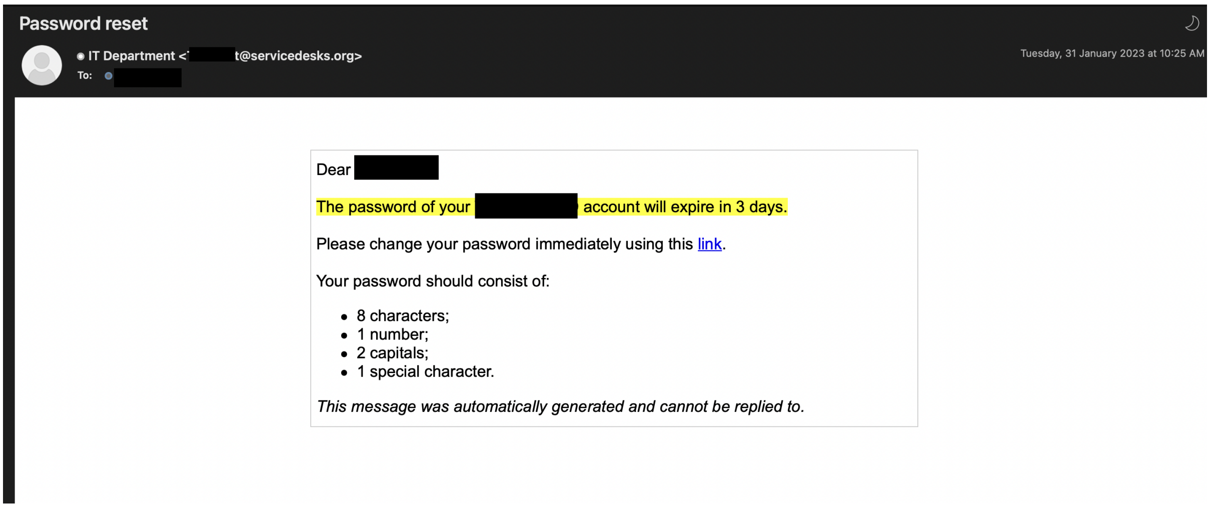
[redacted]

Use a different account

Activate Office

This is an automatic generated email, you can not respond on this email address.

Figure 16: Phishing Simulation Email Round 1



Password reset

IT Department <[redacted]t@servicedesks.org>

To: [redacted]

Tuesday, 31 January 2023 at 10:25 AM

Dear [redacted]

The password of your [redacted] account will expire in 3 days.

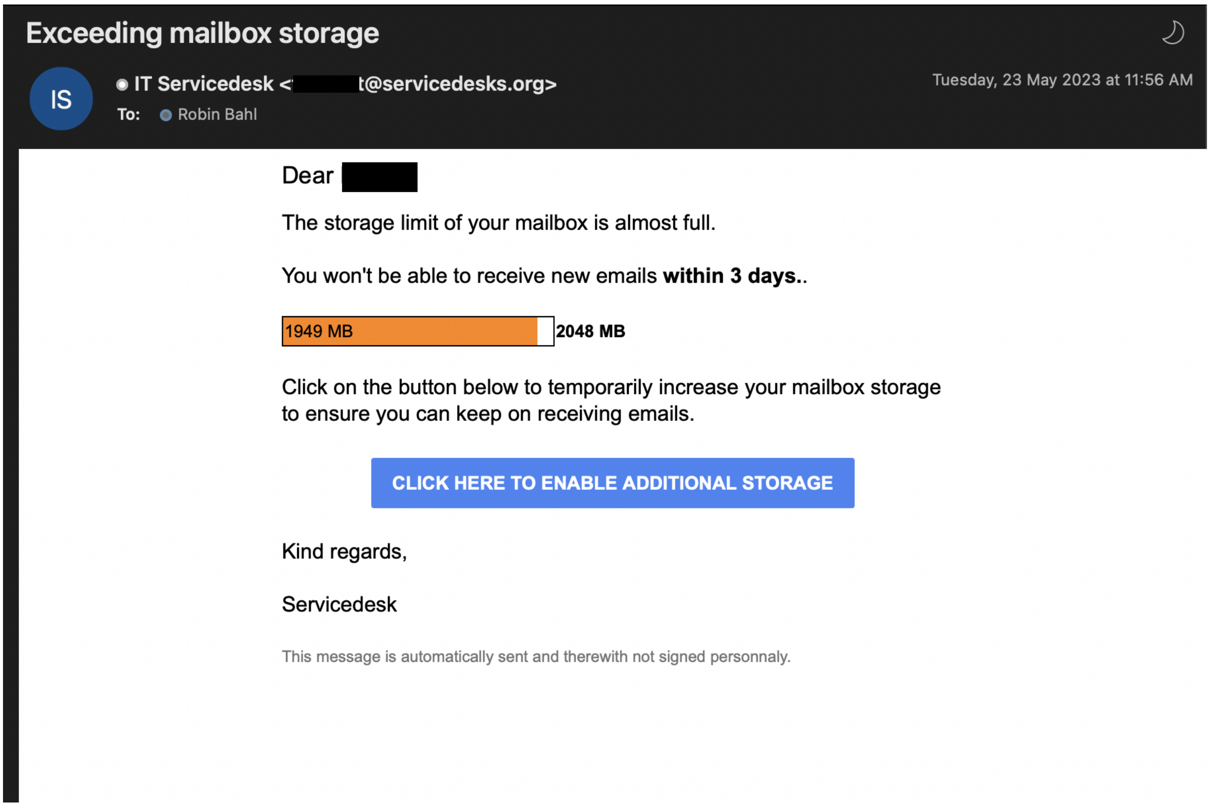
Please change your password immediately using this link.

Your password should consist of:

- 8 characters;
- 1 number;
- 2 capitals;
- 1 special character.

This message was automatically generated and cannot be replied to.

Figure 17: Phishing Simulation Email Round 2



Exceeding mailbox storage

● IT Servicedesk <[redacted]t@servicedesks.org>

To: ● Robin Bahl

Tuesday, 23 May 2023 at 11:56 AM

Dear [redacted]

The storage limit of your mailbox is almost full.

You won't be able to receive new emails **within 3 days.**.

1949 MB **2048 MB**

Click on the button below to temporarily increase your mailbox storage to ensure you can keep on receiving emails.

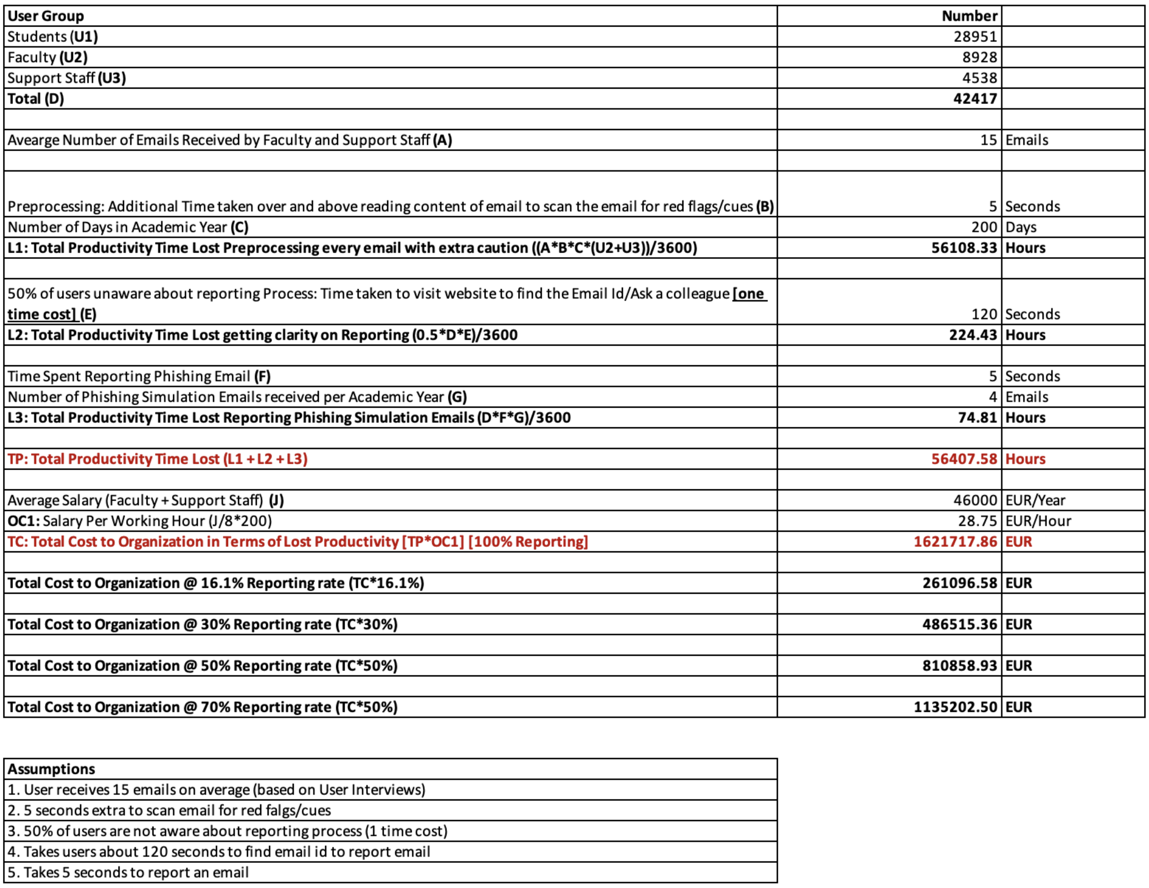
Kind regards,

Servicedesk

This message is automatically sent and therewith not signed personnaly.

Figure 18: Phishing Simulation Email Round 3

A.4 Calculations Cost of Loss Labour Productivity for Organization

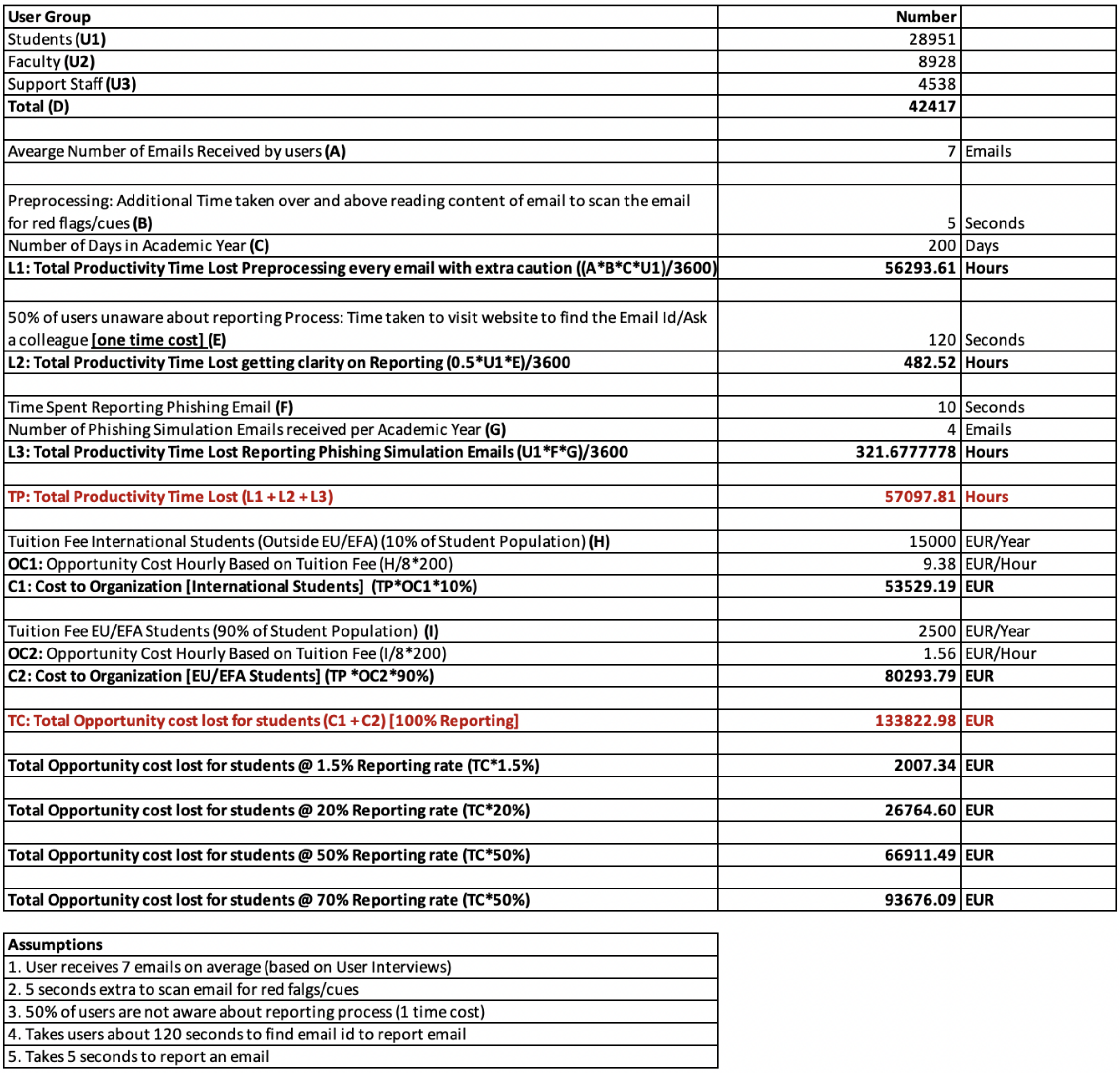


User Group	**Number**	
Students **(U1)**	28951	
Faculty **(U2)**	8928	
Support Staff **(U3)**	4538	
Total (D)	**42417**	
Avearge Number of Emails Received by Faculty and Support Staff **(A)**	15	Emails
Preprocessing: Additional Time taken over and above reading content of email to scan the email for red flags/cues **(B)**	5	Seconds
Number of Days in Academic Year **(C)**	200	Days
L1: Total Productivity Time Lost Preprocessing every email with extra caution ((A*B*C*(U2+U3))/3600)	**56108.33**	**Hours**
50% of users unaware about reporting Process: Time taken to visit website to find the Email Id/Ask a colleague **<u>[one time cost]</u> (E)**	120	Seconds
L2: Total Productivity Time Lost getting clarity on Reporting (0.5*D*E)/3600	**224.43**	**Hours**
Time Spent Reporting Phishing Email **(F)**	5	Seconds
Number of Phishing Simulation Emails received per Academic Year **(G)**	4	Emails
L3: Total Productivity Time Lost Reporting Phishing Simulation Emails (D*F*G)/3600	**74.81**	**Hours**
TP: Total Productivity Time Lost (L1 + L2 + L3)	**56407.58**	**Hours**
Average Salary (Faculty + Support Staff) **(J)**	46000	EUR/Year
OC1: Salary Per Working Hour (J/8*200)	28.75	EUR/Hour
TC: Total Cost to Organization in Terms of Lost Productivity [TP*OC1] [100% Reporting]	**1621717.86**	**EUR**
Total Cost to Organization @ 16.1% Reporting rate (TC*16.1%)	**261096.58**	**EUR**
Total Cost to Organization @ 30% Reporting rate (TC*30%)	**486515.36**	**EUR**
Total Cost to Organization @ 50% Reporting rate (TC*50%)	**810858.93**	**EUR**
Total Cost to Organization @ 70% Reporting rate (TC*50%)	**1135202.50**	**EUR**

Assumptions
1. User receives 15 emails on average (based on User Interviews)
2. 5 seconds extra to scan email for red falgs/cues
3. 50% of users are not aware about reporting process (1 time cost)
4. Takes users about 120 seconds to find email id to report email
5. Takes 5 seconds to report an email

Figure 19: Cost of Loss Labour Productivity for Organization

A.5 Calculation: Lost Opportunity Cost for Students



User Group	**Number**	
Students **(U1)**	28951	
Faculty **(U2)**	8928	
Support Staff **(U3)**	4538	
Total (D)	**42417**	
Avearge Number of Emails Received by users **(A)**	7	Emails
Preprocessing: Additional Time taken over and above reading content of email to scan the email for red flags/cues **(B)**	5	Seconds
Number of Days in Academic Year **(C)**	200	Days
L1: Total Productivity Time Lost Preprocessing every email with extra caution ((A*B*C*U1)/3600)	**56293.61**	**Hours**
50% of users unaware about reporting Process: Time taken to visit website to find the Email Id/Ask a colleague **[one time cost] (E)**	120	Seconds
L2: Total Productivity Time Lost getting clarity on Reporting (0.5*U1*E)/3600	**482.52**	**Hours**
Time Spent Reporting Phishing Email **(F)**	10	Seconds
Number of Phishing Simulation Emails received per Academic Year **(G)**	4	Emails
L3: Total Productivity Time Lost Reporting Phishing Simulation Emails (U1*F*G)/3600	**321.6777778**	**Hours**
TP: Total Productivity Time Lost (L1 + L2 + L3)	**57097.81**	**Hours**
Tuition Fee International Students (Outside EU/EFA) (10% of Student Population) **(H)**	15000	EUR/Year
OC1: Opportunity Cost Hourly Based on Tuition Fee (H/8*200)	9.38	EUR/Hour
C1: Cost to Organization [International Students] (TP*OC1*10%)	**53529.19**	**EUR**
Tuition Fee EU/EFA Students (90% of Student Population) **(I)**	2500	EUR/Year
OC2: Opportunity Cost Hourly Based on Tuition Fee (I/8*200)	1.56	EUR/Hour
C2: Cost to Organization [EU/EFA Students] (TP *OC2*90%)	**80293.79**	**EUR**
TC: Total Opportunity cost lost for students (C1 + C2) [100% Reporting]	**133822.98**	**EUR**
Total Opportunity cost lost for students @ 1.5% Reporting rate (TC*1.5%)	**2007.34**	**EUR**
Total Opportunity cost lost for students @ 20% Reporting rate (TC*20%)	**26764.60**	**EUR**
Total Opportunity cost lost for students @ 50% Reporting rate (TC*50%)	**66911.49**	**EUR**
Total Opportunity cost lost for students @ 70% Reporting rate (TC*50%)	**93676.09**	**EUR**

Assumptions
1. User receives 7 emails on average (based on User Interviews)
2. 5 seconds extra to scan email for red falgs/cues
3. 50% of users are not aware about reporting process (1 time cost)
4. Takes users about 120 seconds to find email id to report email
5. Takes 5 seconds to report an email

Figure 20: Lost Opportunity Cost for Users

A.6 Interview Protocol:

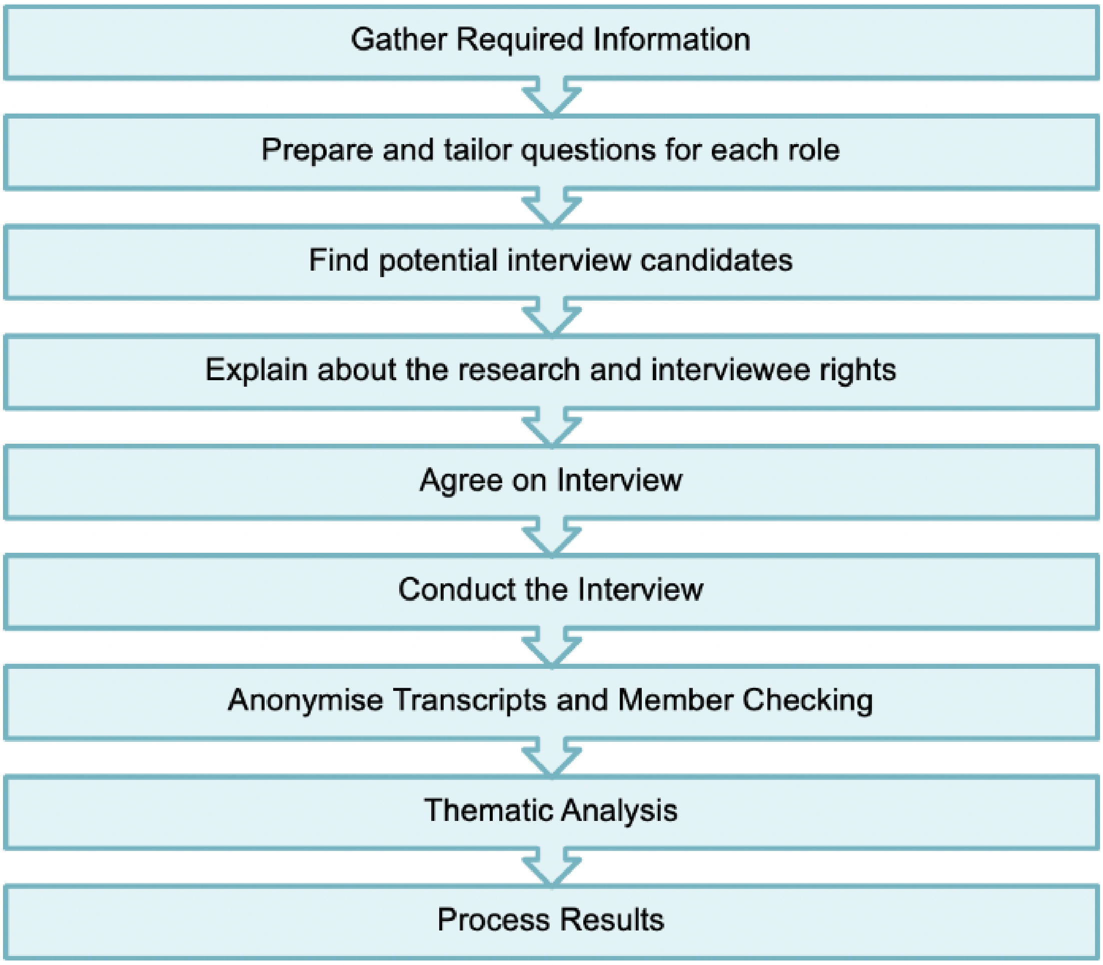
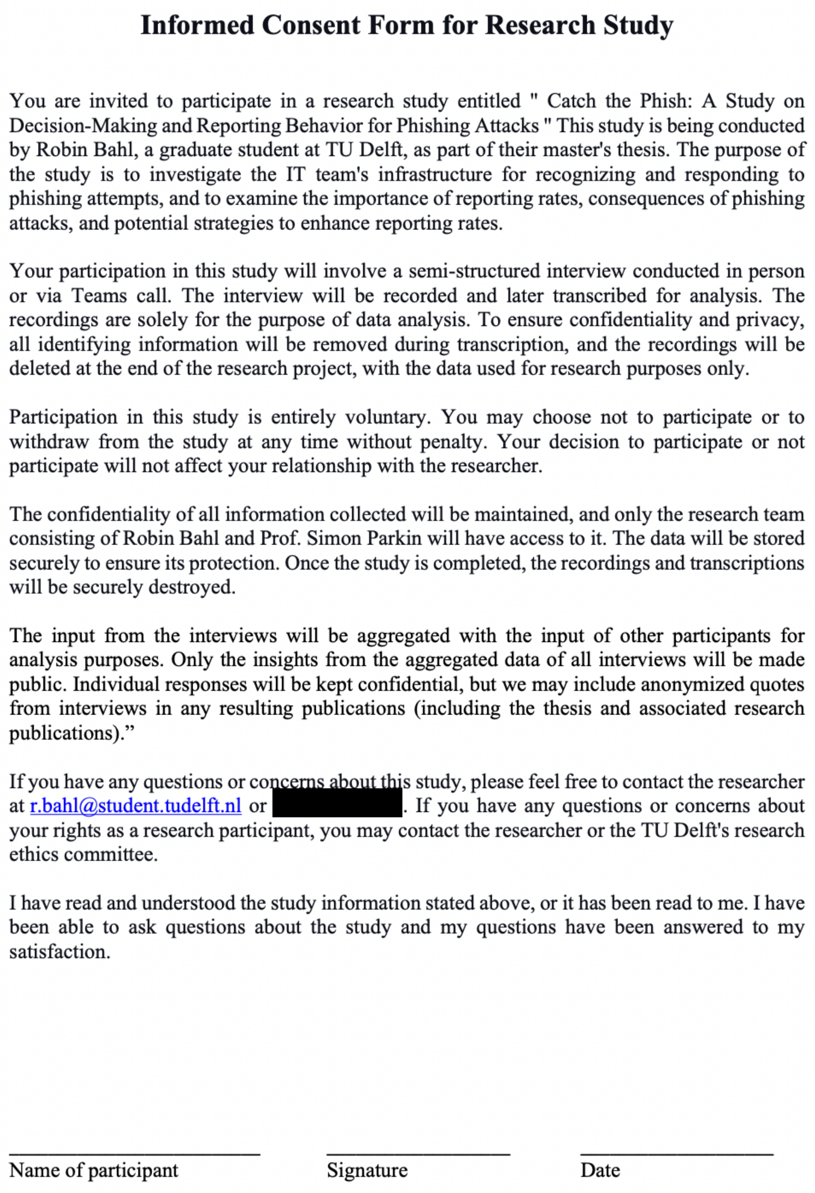

Gather Required Information
Prepare and tailor questions for each role
Find potential interview candidates
Explain about the research and interviewee rights
Agree on Interview
Conduct the Interview
Anonymise Transcripts and Member Checking
Thematic Analysis
Process Results

Figure 21: Interview Protocol

A.7 Consent Forms



Informed Consent Form for Research Study

You are invited to participate in a research study entitled " Catch the Phish: A Study on Decision-Making and Reporting Behavior for Phishing Attacks " This study is being conducted by Robin Bahl, a graduate student at TU Delft, as part of their master's thesis. The purpose of the study is to investigate the IT team's infrastructure for recognizing and responding to phishing attempts, and to examine the importance of reporting rates, consequences of phishing attacks, and potential strategies to enhance reporting rates.

Your participation in this study will involve a semi-structured interview conducted in person or via Teams call. The interview will be recorded and later transcribed for analysis. The recordings are solely for the purpose of data analysis. To ensure confidentiality and privacy, all identifying information will be removed during transcription, and the recordings will be deleted at the end of the research project, with the data used for research purposes only.

Participation in this study is entirely voluntary. You may choose not to participate or to withdraw from the study at any time without penalty. Your decision to participate or not participate will not affect your relationship with the researcher.

The confidentiality of all information collected will be maintained, and only the research team consisting of Robin Bahl and Prof. Simon Parkin will have access to it. The data will be stored securely to ensure its protection. Once the study is completed, the recordings and transcriptions will be securely destroyed.

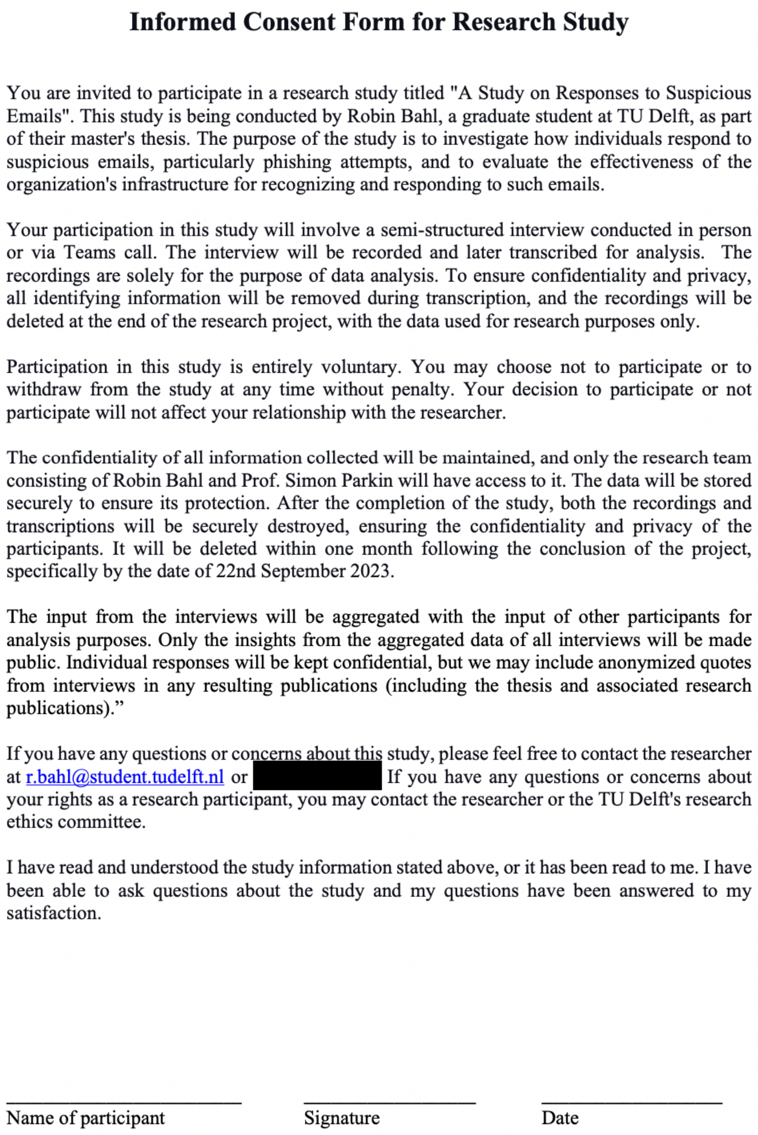
The input from the interviews will be aggregated with the input of other participants for analysis purposes. Only the insights from the aggregated data of all interviews will be made public. Individual responses will be kept confidential, but we may include anonymized quotes from interviews in any resulting publications (including the thesis and associated research publications)."

If you have any questions or concerns about this study, please feel free to contact the researcher at r.bahl@student.tudelft.nl or [redacted]. If you have any questions or concerns about your rights as a research participant, you may contact the researcher or the TU Delft's research ethics committee.

I have read and understood the study information stated above, or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.

______________________ ________________ _________________
Name of participant Signature Date

Figure 22: User Consent Form



Informed Consent Form for Research Study

You are invited to participate in a research study titled "A Study on Responses to Suspicious Emails". This study is being conducted by Robin Bahl, a graduate student at TU Delft, as part of their master's thesis. The purpose of the study is to investigate how individuals respond to suspicious emails, particularly phishing attempts, and to evaluate the effectiveness of the organization's infrastructure for recognizing and responding to such emails.

Your participation in this study will involve a semi-structured interview conducted in person or via Teams call. The interview will be recorded and later transcribed for analysis. The recordings are solely for the purpose of data analysis. To ensure confidentiality and privacy, all identifying information will be removed during transcription, and the recordings will be deleted at the end of the research project, with the data used for research purposes only.

Participation in this study is entirely voluntary. You may choose not to participate or to withdraw from the study at any time without penalty. Your decision to participate or not participate will not affect your relationship with the researcher.

The confidentiality of all information collected will be maintained, and only the research team consisting of Robin Bahl and Prof. Simon Parkin will have access to it. The data will be stored securely to ensure its protection. After the completion of the study, both the recordings and transcriptions will be securely destroyed, ensuring the confidentiality and privacy of the participants. It will be deleted within one month following the conclusion of the project, specifically by the date of 22nd September 2023.

The input from the interviews will be aggregated with the input of other participants for analysis purposes. Only the insights from the aggregated data of all interviews will be made public. Individual responses will be kept confidential, but we may include anonymized quotes from interviews in any resulting publications (including the thesis and associated research publications)."

If you have any questions or concerns about this study, please feel free to contact the researcher at r.bahl@student.tudelft.nl or [redacted] If you have any questions or concerns about your rights as a research participant, you may contact the researcher or the TU Delft's research ethics committee.

I have read and understood the study information stated above, or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.

________________________ ________________ ________________

Name of participant Signature Date

Figure 23: ICT Team Consent Form

A.8 User Interview Questionnaire

1. Can you tell me about your understanding of phishing?

2. Are you concerned about phishing attacks and their impact on your work/organization? If yes, what do you think are the potential consequences?

3. Have you ever encountered a suspicious email that you suspected to be a phishing attempt? If yes, please describe that experience/thought process. What steps did you take?

4. In your opinion, whose responsibility do you believe it is to stop phishing attacks?

5. How confident are you in your ability to identify phishing emails?

6. Have you ever reported a phishing email? What factors influence your decision to report or not report a suspicious email as a potential phishing attempt?

7. Can you share any specific barriers or challenges you face when it comes to reporting phishing emails? What resources, tools, or support mechanisms would you find helpful in increasing your confidence and ability to report phishing emails effectively?

8. How would you describe your experience with phishing simulation exercises and the reporting process in the university/organization?

9. What are your thoughts on the role of incentives in motivating individuals to report phishing emails? Do you believe incentives would be effective? Why or why not?

A.9 ICT Team Interviews

Abuse Team:

- Can you describe the process for handling reported phishing emails?
- How has the volume of reported phishing emails changed over time?
- How do you prioritize which reported emails to investigate?
- What challenges do you face in identifying and investigating phishing emails and what tools/techniques do you use to overcome this?
- How do you communicate with the user who reported a phishing email?
- Can you walk me through a recent successful phishing incident and how it was handled?
- How do you determine whether a reported email is a legitimate threat or a false positive?
- How effective do you believe the current infrastructure and processes are in place for identifying and reporting phishing emails?
- In your opinion, what improvements could be made to the current reporting system?
- What role do you think training and awareness programs play in promoting secure behavior in response to phishing attacks?
- How do you think reporting rates could be improved, and what steps could be taken to encourage individuals to report suspected phishing emails?
- What do you think are the most important factors to consider when developing infrastructure and processes to combat phishing attacks?

Security Manager:

- What is the organization's overall strategy for preventing and responding to phishing attacks?
- How do you prioritize security investments and resources to combat phishing attacks?
- Can you walk me through a recent successful phishing incident and how it was handled?
- How do you balance the need for security with the need for employee productivity and ease of use of technology tools?
- How do you measure the effectiveness of the current infrastructure for identifying and reporting phishing emails?
- How do you communicate security risks and policies to employees?

- What process do you follow for evaluating and implementing new security solutions for phishing prevention?
- How do you ensure collaboration between the different teams to improve the overall security posture of the organization?
- How do you plan for and manage security incidents related to phishing attacks?
- How do you ensure that the organization's security strategy is up to date with the latest phishing tactics?
- In your opinion, what improvements could be made to the current reporting system?
- What do you think are the main reasons that individuals fail to report phishing emails?
- How do you think reporting rates could be improved, and what steps could be taken to encourage individuals to report suspected phishing emails?
- What role do you think training and awareness programs play in promoting secure behavior in response to phishing attacks?

Privacy Team: (Legal, Contracts & IT - Technical solutions/ GDPR)

- What are the consequences of successful phishing attacks in terms of user privacy and data security?
- How do you respond to a successful phishing attack that may have resulted in a data breach?
- How do you communicate with affected individuals and stakeholders in the event of a successful phishing attack?
- What steps do you take to prevent data breaches resulting from phishing attacks?
- Can you walk me through a recent successful phishing incident and how it was handled?
- What challenges do you face in identifying and responding to privacy risks related to phishing attacks?
- How do you collaborate with other teams, such as the Abuse Team and Security Manager, to mitigate privacy risks related to phishing attacks?
- How effective do you believe the current infrastructure and processes are in place for identifying and reporting phishing emails?
- What do you think are the main reasons that individuals fail to report phishing emails?
- How do you think reporting rates could be improved, and what steps could be taken to encourage individuals to report suspected phishing emails?

- What do you think are the most important factors to consider when developing infrastructure and processes to combat phishing attacks?
- What role do you think training and awareness programs play in promoting secure behavior in response to phishing attacks?

Phishing Simulation Provider

- How do you design your phishing simulation exercises?
- What are the specific characteristics that make a phishing email effective?
- How do you measure the success of a phishing simulation exercise?
- Can you provide examples of successful and unsuccessful phishing simulation exercises that you have run in the past?
- How often do you recommend running phishing simulation exercises?
- How do you tailor your phishing simulation exercises to different types of users or departments within an organization?
- How do you ensure the privacy and security of user data during a phishing simulation exercise?
- What are the best practices for conducting a phishing simulation exercise, from planning to execution?
- How do you handle user responses and feedback to a phishing simulation exercise?
- What are the most common mistakes that organizations make when designing or conducting phishing simulation exercises?
- What do you think are the main reasons that individuals fail to report phishing emails?
- How do you think reporting rates could be improved, and what steps could be taken to encourage individuals to report suspected phishing emails?
- What do you think are the most important factors to consider when developing infrastructure and processes to combat phishing attacks?
- What role do you think training and awareness programs play in promoting secure behavior in response to phishing attacks?

Technical Solution Provider

- How does your solution identify and filter out phishing emails?
- What are the specific features or technologies that make your solution effective in detecting and preventing phishing attacks?

- How does your solution adapt to new and evolving phishing techniques?
- How does your solution handle false positives and false negatives?
- How does your solution integrate with an organization's existing security infrastructure?
- How does your solution handle different types of phishing attacks, such as spear phishing or whaling?
- How do you measure the effectiveness of your solution in detecting and preventing phishing attacks?
- How often do you update your solution's algorithms or features to keep up with new threats?
- Can your solution provide real-time alerts or notifications for potential phishing attacks?
- How do you ensure the privacy and security of an organization's email data while using your solution?
- How does your solution handle phishing attacks that originate from internal sources, such as compromised user accounts?
- What do you think are the most important factors to consider when developing infrastructure and processes to combat phishing attacks?
- What role do you think training and awareness programs play in promoting secure behavior in response to phishing attacks?