A Study on The Effectiveness of Education and Fear Appeal to Prevent Spear Phishing of Online Users

Saja Alsulami

A thesis
submitted in partial fulfillment of the
requirements for the degree of

Master of Science

University of Washington

2024

Reading Committee:
Marc Dupuis, Chair
Arkady Retik
William Lidster

Program Authorized to Offer Degree:
Cybersecurity Engineering

University of Washington

Abstract

A Study on The Effectiveness of Education and Fear Appeal to Prevent Spear Phishing of Online Users

Saja Alsulami

Chair of the Supervisory Committee:
Marc Dupuis
Department of Computing & Software Systems

Spear phishing attacks are considered one of the most elaborate forms of social engineering. It presupposes that an attacker designs a scam to obtain the personal information of specific users from their social media accounts. It involves a preliminary analysis of targeted users and their online behaviors needed to persuade them that a malicious link or attachment is sent by a trusted person. This attack implies that human beings are the weakest link within a security system; their vulnerabilities could be exploited. The most detrimental consequences following spear phishing attacks are financial losses, network compromises, loss of login credentials, and malware installation.

This quantitative study used Protective motivated theory (PMT) to examine the impact of education and fear appeals on users' knowledge and abilities to identify spear phishing attacks. Three interventions were implemented: an education intervention, a fear appeal intervention, and a combined education and fear appeal intervention. The control group was used for comparison purposes. This study was conducted as an online experiment that was managed via the Qualtrics platform. It has 726 participants, and they were assigned randomly into four groups; after interventions, there was a spear phishing test to evaluate their knowledge and abilities to identify spear phishing attacks. The spear phishing test was administered to compare the efficacy of every intervention group (education, fear appeal,

and combined education and fear appeal) to the control group. The experiment findings revealed no statistically significant differences in the mean test for these four groups. The PMT finding revealed that the high effect of threat vulnerability, self-efficacy, and the low effect of cost response can enhance the participant's knowledge of spear phishing attacks. The study results indicate further research is needed to develop an effective intervention program that would considerably enhance users' knowledge of spear phishing attacks and their resilience to them.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GLOSSARY

AVE: Average

HIT: Human Intelligence Task

HTMT: Heterotrait-monotrait ratio

PMT: Protection Motivation Theory

RCT: Randomized controlled trial

SETA: Security Education, Training, and Awareness

SPSS: Statistical Package for the Social Sciences

SMARTPLS: Smart Partial Least Square

ACKNOWLEDGMENTS

I am grateful to my family for their unwavering support. To my dad, mom, sisters, and brothers, thank you for your constant help and love.

I would also like to express my heartfelt thanks to my advisors, Dr. Marc Dupuis, Dr. Arkady Retik, and Dr.William Lidster, for their invaluable guidance and support throughout my journey. I have learned so much from you.

DEDICATION

To my Dad, thank you. You worked so hard for our family to give us love and support.

To my Mom, thank you for your love, patience, and your sacrifice.

To my sister Ebtehage, thank you so much for your support; I am so happy to have you in my life.

To my brother Hamzah, thank you for your help and unlimited support. Your encouragement has meant so much to me.

To Yhya, thank you for your patience and support.

To the rest of the family, thank you.

To my committee, Dr.Marc Dupuis, Dr.Arkady Retik, and Dr.William Lidster thank you for your invaluable guidance and support throughout my journey.

Chapter 1

INTRODUCTION

Spear phishing is using email and electronic communication that explicitly targets individuals within a company or organization intending to steal sensitive data such as bank details and login details or install a virus on the recipient's computer [82]. Spear phishing is less in number and more specific compared to regular phishing. It creates an email account to target a few users, and the content consists of a malicious link or file. Spear phishing generally entails an extensive effort to make the fake message look authentic [151]. This kind of assault predominantly focuses on accessing sensitive information from an organization or extorting cash from the firm and its leaders [11]. According to Stajano and Wilson (2015), spear phishing attacks commonly achieve their goal due to the focus on human factors. The attacker gets the trust of the victim through impersonation by portraying to be a trustworthy coworker or organization, and this makes the victim likely to open up to sharing their secrets or even clicking on dangerous links [190]. To decrease the possibility of being a victim of spear phishing attacks, the study highlights the necessity of providing security awareness training and solid technological defenses [191].

Recently, institutions have prioritized comprehensive training programs that increase knowledge regarding cybercriminals' typical strategies to effectively combat spear phishing [74, 196]. By training students, faculty, employees, and staff to identify suspicious emails, avoid clicking on malicious links, and report potential threats, the institutions can substantially decrease the likelihood of becoming a target of spear phishing attacks [80].

On the other hand, the fear appeal approach creates awareness among users, creating fear so that users will take measures to avoid becoming victims of spear phishing attacks [176]. Fear appeal is a persuasive communication strategy aimed at motivating individuals to take

action by emphasizing the potential negative consequences of inaction [127]. A fear appeal can be an impactful method for increasing awareness about the risk of falling victim to such attacks [95]. Organizations can create a sense of urgency and make individuals adopt security practices by highlighting real-world examples and the impacts of spear phishing, such as financial losses, data breaches, and reputational damage [45]. However, balancing producing fear with providing practical guidance to empower individuals to protect themselves effectively against spear phishing attacks is crucial [119].

Spear phishing attacks exploit system vulnerabilities, whether these stem from technical weaknesses or a lack of knowledge among users [17]. Thus, researchers develop defenses against such attacks based on technical awareness, focusing on users and utilizing educational material that includes spear phishing attacks and how to avoid them. Various strategies have been explored to address spear phishing while enhancing awareness and educating users. Spear phishing attempts seek to illegally obtain confidential information from victims, often resulting in significant financial loss [6]. Research indicates that a third of phishing attempts in 2013 targeted bank accounts or pursued other financial data [80]. Spear phishing is a serious risk to humans and companies since a successful attack might have expensive and far-reaching effects. To identify and minimize these attacks, people must continue being alert and suspicious of emails and electronic communications.

1.1 Research Subject

Recently, individuals and organizations increasingly depend on electronic communication, which makes humans susceptible to social engineering attacks [4]. Social engineering attacks represent one of the biggest threats to individuals' and organizations' information security because they explore human vulnerability [125]. Social engineering is an attack when the attacker collects information for target users and utilizes that to launch an attack on a specific user. The growth in social engineering implies that extensive social media accounts offer new possibilities for exploiting humans' vulnerabilities; this has led security experts to recognize human behavior as a weak link in security systems [126]. Social engineering is a highly

effective strategy for taking advantage of human susceptibility, mainly through phishing attacks [39]. In these attacks, attackers deceive victims into performing unintended actions by pretending to be legitimate actors, often using direct messaging platforms like email for solicitation In these attacks, attackers pretend to be legitimate actors to deceive victims into performing actions, often using direct messaging platforms like email for solicitation [183].

Phishing, a subtype of social engineering, utilizes messaging platforms like email to distribute attacks. Today, many people and employees use emails to send official documents, receive notifications from banks, and send updates on their work to their employers. Many people trust emails because they can send encrypted content, but they are often unaware that they may be victims of the attack [159]. The employee's vulnerability to spear phishing attacks has led researchers to emphasize technical training programs that include examples and indicators for social engineering attacks [13]. For instance, surveys within the industry indicate that employee security awareness training programs are essential to protect information, and chief information security officers highlight employee training as a crucial component of an effective security strategy [217].

This study is motivated by previous studies on training effectiveness and fear appeals. It focuses on the importance of online user training in preventing people from becoming victims of spear phishing strategies [74, 196]. This study aims to assist online users by developing practical training initiatives that decrease users' vulnerability to spear phishing attacks. This study utilized an experiment involving four intervention groups to assess the impact of the developed training on online users' knowledge and ability to identify spear phishing attacks.

1.2 Problem Statement

Security systems have many components that affect them, from users to network configurations. No matter how robust a firewall or advanced data encryption and antivirus software are, human error presents the greatest vulnerability of any security system [74]. This study tackles the problem of the increased risk that human error poses to systems [128]. It is crucial to work on the guidelines for evaluating losses and mitigating the threats of spear

phishing as the usage of the internet increases and people rely on digital platforms more and more for different activities [48]. Therefore, this study is designed training might be efficient and preventive with the help of researching the effectiveness of fear appeals and education approaches.

1.3 Methodology

This study applies a quantitative research strategy [21]. Therefore, the experiments managed via survey instruments were developed to assess the impact of using education training and employing fear appeals against spear phishing attacks. The instrument includes four experiments. The various interventions were tried on different subjects.

The first study is education intervention, the second is fear appeal, and the third is a combination of education and fear appeal. The fourth is the control group, which contains individuals who do not engage in any interventions. All the survey experiments for all groups include the same questions but different kinds of intervention.

The first group is exposed to cybersecurity education and training modules about spear phishing attacks. Education intervention comprised images and videos to improve participants' understanding of these categories of attacks [50]. The second group of participants was exposed to fear appeal communication scenarios. The fear appeal scenarios used were intended to create a sense of urgency and underscore the risks posed by spear phishing threats. This intervention involves a video on the consequences of spear phishing attacks [175]. The third group combined education and fear appeal interventions. The education and fear appeal approach combined the advantages of both methods and offered the participants training focused on both elements: the knowledge of the issue and the necessity of being afraid of spear phishing attacks. The fourth group is the control group, which does not have spear phishing effects [66]. At the end of the interventions, the participants are given a Protective motivated theory (PMT) Constructs and spear phishing test to assess their understanding of spear phishing attacks.

The quantitative data used in this study will be analyzed using Statistical Package for

the Social Sciences (SPSS) version 29. 0. 1. 0 and SmartPLS for data analysis [150].

1.4 Research Questions and Hypotheses

This study aims to measure the effect of four interventions: the education group, the fear appeal group, a combination of education and fear appeal group, and the control group.

• Research Question: What is the effect of education, fear appeals, and combined education and fear appeal interventions on participants' knowledge for identifying spear phishing and legitimate emails compared to a control intervention?

To examine the effect of the intervention on each group and the control group, the study will test three hypotheses for this research question.

H1: Higher levels of education intervention have a high effect on users' knowledge for identifying spear phishing attacks compared to the control group.

H2: Higher levels of fear appeal intervention have a high effect on users' knowledge for identifying spear phishing attacks compared to the control group.

H3: Higher levels of a combination of education and fear appeal intervention have a high effect on users' knowledge for identifying spear phishing attacks compared to the control group.

• Research Question: How does the PMT (threat severity, vulnerability, response efficacy, self-efficacy, and response costs) affect users' knowledge for identifying spear phishing and legitimate emails?

H4: Higher level of threat severity is associated with higher levels of performance in the spear phishing test.

H5: Higher level of threat vulnerability is associated with higher levels of performance in the spear phishing test.

H6: Higher level of response efficacy is associated with higher levels of performance in the spear phishing test.

H7: Higher level of self-efficacy is associated with higher levels of performance in the spear phishing test.

H8: Lower response cost is associated with higher levels of performance in the spear phishing test.

1.5 Research Aim

The research objectives are as follows: The research seeks to assess the efficiency of education, fear appeals, and preventive measures in minimizing spear phishing among online users. This research is crucial since it presents two approaches for establishing the impact of their enhancement on the users' awareness levels and, consequently, their susceptibility to spear phishing attacks.

The study has the following objectives:

• Evaluate the impact of education programs on increasing users' awareness and knowledge of spear phishing attacks.

• Assess the effectiveness of the fear appeal approach in users' behavior when facing spear phishing attacks.

• Examine the impact of a combination of education and fear appeal on users' susceptibility to spear phishing.

• Examine the impact of PMT constructs on users' knowledge of spear phishing attacks.

1.6 Nature of the Study

This study uses a quantitative research method to address the problem of human factors in security [14]. The study considers spear phishing attacks to be widespread social engineering attacks. This study adopts an experimental research design to investigate the effectiveness of education, fear appeal, and a combination of education and fear appeal interventions among online users. The research employs adapted education and fear appeal intervention content and questions from a prior study that tested and assessed for validity and reliability. [201].

This study targeted end users, including individuals, employees, students, and faculty. It used an experiment with four interventions. The participants were assigned randomly to the

education, fear appeal, combination of education and fear appeal, and control groups. The experiment was administered via the Qualtrics survey platform.

1.7 Definition of Key Terms

This section seeks to provide the meaning of the terms used in this study.

• Spear phishing is a specific type of phishing attack where fraudsters target specific individuals within an organization with emails or messages that appear legitimate to obtain personal details [156].

• Education involves teaching people knowledge, skills, and information to improve their comprehension and capacity to prevent spear phishing attacks [75].

• Fear appeal is a persuasive communication approach that aims to induce anxiety or fear in people to motivate them to modify their behavior to protect against spear phishing [196].

• Effectiveness means the level to which education and fear appeal initiatives accomplish the targeted results of spear phishing prevention, such as gains in awareness, knowledge, and behavioral improvements [142].

• Online users conduct online activities like searching, sending emails, or communicating on social media, and they may be the target of spear phishing attacks [173].

1.8 Conclusion

Many attacks have been optimized to exploit human vulnerability, the weakest link in security systems [23]. Many research studies have used fear appeals or education to affect users and prevent attacks [74, 94]. However, a few research studies have focused on education to avoid spear phishing attacks. This study used a combination of education and fear appeal approaches to inform users about preventing spear phishing attacks.

The remainder of the thesis is organized as follows:

The literature review presents an overview of current research on spear phishing, education, fear appeal, and PMT. This chapter begins by defining spear phishing and its

significance as a prevalent cybersecurity threat. It explains the different studies that used education intervention and fear appeal intervention.

The methodology chapter outlines the approach employed to study the effectiveness of education and fear appeal in preventing spear phishing among online users. It explains the research design, including participants, developing education and fear appeal content, and implementing the experimental procedures. Additionally, the chapter explains ethical considerations, data collection methods, and statistical analyses utilized to evaluate the effectiveness of education and fear appeal interventions.

The results and discussion chapter presents the findings, followed by discussions and interpretations. It begins by summarizing the quantitative data obtained from the spear phishing test to identify spear phishing and legitimate emails. The conclusion explains the limitations and future work and also includes the conclusion.

Chapter 2

LITERATURE REVIEW

Phishing attacks have appeared as a pervasive and challenging threat, which makes security risk for organizations and individuals [37, 80]. These attacks exploit human vulnerabilities, like a lack of social engineering techniques, making them a particularly unique form of cybercrime [13]. Educational programs and fear appeals have been developed to reduce this threat and encourage individuals to recognize and report phishing scams. However, the effectiveness of these methods remains ambiguous and requires an examination of the methodologies employed in anti-phishing training [99]. This literature review provides insight into current research concerning human factors in cybersecurity, social engineering attacks, phishing, spear phishing, education, and fear appeal, focusing on the multifaceted aspects that influence human efficacy in this domain. This thesis applies fear appeal and education as strategic components of cybersecurity training. Additionally, it explores current trends within this field to offer a background for the research field.

This chapter discusses findings from my review of articles and journals related to the research topic and the existing approaches for enhancing education through training programs and fear appeals against spear phishing. This literature review is structured into sections. Section 2.1 presents the Protection Motivation Theory and the general support for fear appeals. Section 2.2 builds on the concept of employing fear appeals in motivating people to be safe from spear phishing, examining its efficacy. Section 2.3 reflects how human factors may affect security systems. Section 2.4 describes Social Engineering attacks and the methods attackers employ to impact users significantly. Section 2.4.1 provides information about phishing attacks that use different approaches to launch these attacks and includes two sections for the most popular attacks, such as phishing and spear phishing attacks. Section 2.5

provides current educational approaches to design training programs that help improve the user's awareness about security. Section 2.6 provides a comparison of the different methods that have been used in education and fear appeal. Section 2.7 The research gap for this study. Section 2.8 provides a conclusion for this chapter.

I gathered articles, books, and reports from Google Scholar, the University of Washington Library, and several databases such as IEEE Xplore, JSTOR, Science Direct, and EBSCO. I used Search terms including "Spear phishing," "Fear Appeal," "Education," "Awareness," "Effectiveness," "Cybersecurity," "Social Engineering," "Phishing Attacks," and "Human Factor." These varied databases helped me to find several research related to this study.

2.1 Protection Motivation Theory

Protection motivation theory (PMT) is persuasive communication that affects protective behavior. PMT focuses on attention to the cognitive processes that contain fear appeals and behavioral change. Rogers introduced PMT in 1975, aiming to clarify how persuasive messages affect behavior by emphasizing the mental mechanisms determining individuals' decisions to adhere to or disregard recommended behaviors [170]. Initially designed for application in healthcare settings, the theory delves into the cognitive processes shaping individuals' responses to persuasive communication [54].

PMT assumes that the tendency to embrace a suggested behavior results from a mindset influenced by cognitive processes mediating the impact of fear appeals [53]. The theory asserts that protective actions against health threats depend on an individual's drive for self-preservation [71]. The integration of coping and threat appraisal processes contributes to protection motivation. Existing literature indicates that PMT effectively foresaw whether individuals will adopt or avoid protective behaviors [71, 178, 204].

Numerous investigations have employed PMT to understand and predict diverse protective actions, such as physical activity engagement and adherence to COVID-19 preventive measures [43, 71]. Additionally, PMT has been utilized to explore the factors influencing cardiac patients' motivation to maintain a nutritious diet and exercise regularly [160, 130].

PMT has been applied as a model for predicting protective behaviors, and its efficiency has been validated in various situations [43]. In the PMT theory, the motivation is affected by both threat and coping appraisal.

2.1.1 Threat Appraisal

Threat appraisal includes perceived severity (evaluating the level of harm) and perceived vulnerability (assessing the likelihood of occurring harm) while excluding considerations of the perceived rewards (positive aspects) associated with the situation. Standard measures of threat appraisal within PMT typically involve assessing severity and vulnerability [118]. Threat appraisal has also been employed to investigate how inducing fear of obesity impacts the physical activity of young female college students [162]. Moreover, the interplay of threat appraisal and resilience with health behaviors is mediated by problem-solving [112]. Also, House and Raja (2019) study found that individuals who have a high fear appraisal are more likely to take protective action [94, 58].

Threat Severity

Threat severity is an individual's estimate of the harm caused by a threat. It points to the drawbacks of possible severity [134, 76]. For example, during COVID-19, people who perceive that the virus threatens their health result in protective measures such as wearing a face mask and avoiding close contact with others. Furthermore, Rui's work (2021) indicates that perceived severity is positively related to protective action motivation [171].

Threat Vulnerability

Threat vulnerability is used to reason about alert actions to people across various domains like information security, health, and privacy [3, 59, 97]. Perceived vulnerability is defined as an individual's evaluation of the possibility of a threat to occur [3]. In this respect, Destici's (2015) work identified the influence of perceived threats in privacy protection, such as

customizing privacy settings on social networking services [59]. In addition, Abdul Hameed aggregated a review of 38 studies that examine the perceived vulnerability effect in adapting behaviors in information system security and privacy protection for individual and organizational contexts [3].

2.1.2 Coping Appraisal

Coping appraisal combines the assessment of response efficacy (the users perceived the effectiveness of recommended behavior in minimizing the threat), self-efficacy (the users perceived their ability to apply the recommended behavior), and response cost (the user perceived the cost associated with the protective action) [127].

Perceived Response Efficacy

Response efficacy provides insights into how individuals react to fear appeals to encourage different behaviors. It indicates the belief that adopting the recommended response will effectively reduce the perceived threat [104]. Bigsby's (2022) study analyzes 158 studies on the effect of fear appeals on behavioral outcomes, specifically when they incorporate positive response efficacy information [34]. Therefore, response efficacy is an adequate scale in influencing behavior change and should be a consideration in designing impactful health communication messages [171]. Additionally, research indicates a connection between response efficacy and self-efficacy. The interventions that support response efficacy and self-efficacy have proven more successful in fostering behavior change than those targeting only one of these factors [211].

Self Efficacy

Self-efficacy measures individuals' ability and confidence to do a recommended behavior to protect themselves from the threat. Self-efficacy approaches are applied in health, education, and psychology. [127]. In security, self-efficacy plays a significant role in shaping individu-

als' behaviors and practices concerning information security and privacy [166]. In addition, Clarke's (2010) study has delved into the connection between self-efficacy and security behaviors, particularly within computer and information security. The study indicates that self-efficacy in information security significantly explains individuals' behavior in practicing information security behaviors [51].

Additionally, one's belief in their capability to execute IT security or privacy skills, cybersecurity self-efficacy, has emerged as a motivational factor that significantly impacts individual security behaviors [145]. The significance of self-efficacy in security is underscored by its influence on the technology-to-performance chain model, where it extends and examines the link between computer security self-efficacy and security performance [10]. Consequently, self-efficacy is crucial in various domains, underscoring its importance in crafting effective security measures and interventions [23]. Self-efficacy is a vital concept studied across multiple disciplines, reflecting its substantial influence on individuals' behaviors and experiences [34].

Perceived Response Costs

Response cost is the efforts associated with operating protective behaviors. For example, the cost of time, money, energy, or any other resources an individual must use to adopt a protective behavior. In PMT, a higher cost response can lead to a lower level of coping appraisal, as protective behaviors are less likely to be employed. If individuals believe that there are high costs associated with protective behaviors, such behaviors may not be used frequently by such people [170]. To decrease the response costs and increase the chances that individuals will change their behavior, they should be supplied with the tools that can help apply the costs of protective behaviors. Moreover, educating persons on why protective behaviors are beneficial may assist them in being more inclined to engage in such behavior [29]

2.2 Fear Appeal in Cybersecurity

Fear appeal is one of the persuasion techniques that influence users 'behavior using the principles of psychology. It has been analyzed in psychology in detail. Fear appeal is composed of close messages that seek to elicit fear in the audience by depicting the potential harm and risk of not adhering to instructions given in the message [63, 188]. The fear appeal comprises the consequences of using or not using a specific service that may result in certain adverse outcomes [207]. Many research articles have been presented on fear appeals and their influence on attitudes, intentions, and behaviors [102, 196]. Hence, attitude and behavior have also been pointed out when studying how a potential victim might be apprehended in a phishing attack, even as technologies for avoiding such attacks have been pointed out [120].

2.2.1 Fear Appeal Effect

Contemporary security studies have examined how fear appeals influence a user's capability to guard against risks. House and Raja (2020) focused on the analysis of the effects of fear appeal coupled with self-confidence in participants who were targeted for phishing attacks. They discovered that 18% of the users who clicked a phishing link perceived more fear, meaning a decreased probability of the subject clicking on the link [96]. In addition, Jansen and Schaik (2017) presented three different fear appeal scenarios to 1,201 Internet users; the strong fear appeal condition led to increased assessments of the threat, coping appraisal, and motivation to protect against phishing attacks [101].

Furthermore, an online study involving 1,486 participants determined that adjusting a specific warning message to be visual and noticeable can improve the percentage of individuals who take protective action by approximately 65% [68]. Also, Johnston, et al.(2010) study findings indicate that fear appeals influence users by encouraging them to follow guidelines for security practices, but the extent of this influence varies; this variation is influenced by factors such as self-confidence, the perceived effectiveness of their response, the severity of the threat, and social impact [104]. Tannenbaum (2015) investigated predictions based on

a wide range of hypotheses from 127 papers, resulting in 248 independent samples. The research findings indicated that incorporating efficacy statements into fear appeals greatly impacted users' intentions, attitudes, and behaviors [196]. However, Lawson et al. (2016) discovered that employing extremely fearful messages without providing clear and practical guidance on addressing the threat is counterproductive and reduces motivation to take action. Therefore, concerns about using scenarios in cybersecurity are valid as they could deter efforts to encourage appropriate policy responses to real cyber threats [119]. Also, a study examining the effect of fear on users' behaviors found that the message affects the users if repeated three times [182]. In addition, Ray and Wilkie (1970) found that solid fear led to harmful actions such as avoiding a message or deleting it [161].

It is essential to explore the effect of fear appeal on attacks to motivate users to protect themselves against spear phishing attacks. The fear appeal approach strives to prepare and protect users when they encounter an attack by making them feel at risk if they do not respond to the attack recommendation [104]. Utilizing fear appeals to modify behavior against phishing attacks [95]. By understanding how fear appeals impact an individual's reaction to phishing attacks, researchers and organizations can create efficient anti-phishing training programs rooted in fear appeals. These programs aim to make users aware and stimulate their motivation for protection [176].

2.2.2 Factors that Affect Fear Appeal

Researchers have investigated several factors assumed to impact the efficiency of fear appeals, including the message's content, the different behaviors suggested by the message, and the audience's characteristics [196]. Also, low-fear appeal demonstrates an adequate perception that leads to a person's desire to participate in pro-environmental conduct and moral duties [49]. In addition, fear appeal theories indicate that people's personality may affect their coping assessments; for example, people are driven to collect knowledge and pay attention to information, which can ultimately lead to taking protective action [212, 76, 111]. To address the results of previous studies, Schuetz's (2020) study examined how context (individual users

versus organizational users) and the level of message abstraction (abstract versus concrete) influence the outcomes of fear appeals. Three experiments revealed that fear appeals with concrete content produce the desired fear response more effectively than those with abstract content [175].

2.3 Human Factors in Security

Human factors are one of the most vulnerable factors in security systems in individuals, organizations, and companies [103]. The mistakes made by humans are the reason for the growing number of ransomware attacks, data breaches, and cyberattacks; human error is responsible for 95% of all cyberattacks. Despite the automated security measures, malicious individuals still manage to breach targeted systems by taking advantage of human errors through malware, social engineering, spear phishing, and vulnerabilities generated by technology. The prevalence of these human errors in cybersecurity operations demonstrates that relying only on technology is insufficient to eliminate human mistakes [148]. Researchers and experts suggest that the consequences of malicious cyber activities targeting individuals remain an area of research that has not received enough attention [129]. In addition, limited studies investigate the effect of human factors against spear phishing attacks [215].

Human factors determine how people engage with information security and technologies; this contact is frequently adverse to security [155]. Henshel et al. (2016) study concluded that demographic characteristics, such as gender, age, personality, and cultural circumstances, significantly drive an individual's attitude and behavior toward cybersecurity [88]. Additionally, numerous factors impact users' behaviors, skills, and understanding of cybersecurity, in addition to their experiences, perspectives, attitudes, and beliefs [58, 19, 186]. Several articles have delved into the factors that shape human behavior and drive behavior change [26, 65].

Human elements' subjective and complicated nature requires novel approaches to understand their influence on cybersecurity completely [200]. However, the technological perspective and cybersecurity continue to dominate the majority of studies [56]. As a result, this

underscores the importance of a comprehensive approach to understanding human factors in cybersecurity and finding strategies that minimize the risk associated with human factors [128].

2.4 Social Engineering Attacks

Social engineering is a comprehensive term for a wide range of attackers who exploit computers and utilize various tactics to affect users psychologically. Social engineering uses semantic attacks to evade technical defenses by actively manipulating the attributes of objects (platforms, system applications) to deceive the end user instead of launching direct attacks [85]. Social engineering attacks are classified as non-technical hacking attacks since most occur without technical knowledge. Social engineering primarily focuses on exploiting the most vulnerable elements of the security system—humans— by influencing human psychology to gain access to confidential data [125]. These attacks are difficult to detect and eradicate because they are not recognized by current security software systems [33].

Social engineering exploits human behaviors like curiosity, greed, carelessness, and indifference. Social engineering attacks can risk the secrecy, reliability, and accessibility of information [202, 107]. Social engineering attacks are often complicated and targeted, and they utilize various social engineering methods [113]. Social engineering attacks can potentially affect the confidentiality, integrity, and accessibility of data. This underscores the seriousness, as demonstrated by the data breaches at Yahoo and Sony [40]. The breach of Sony Pictures' data had severe consequences, resulting in significant financial losses for Sony, legal and regulatory problems, and the theft of personal information from thousands of employees. The attackers used a combination of tactics, including malware, to infiltrate Sony's network. They had conducted thorough surveillance before the attack, as evidenced by the malware's many predefined host names [193]. The data breach attack highlights the need for robust protection against social engineering attacks that exploit human vulnerabilities through psychological manipulation and deception [14]. The primary sources of social engineering attacks are social networks and email. Among these, phishing and ransomware

stand out as the most influential forms of attacks [77].

2.4.1 Phishing Attacks

Phishing is an effort to trick a person into disclosing private data, including card numbers and bank accounts, by sending them links that take them to a fake website [17]. Phishing attacks are rapidly rising in the cybersecurity world, and they cost billions of dollars in losses annually [177]. The attacker uses a different approach to steal sensitive information and use it to gain financial profit from banks, government, and individual users [17]. Phishing attacks are among the most significant social engineering attacks that have increased in recent years and pose a considerable risk for users [25]. Phishing can be divided into two primary categories. In the first scenario, a potential target receives a fraudulent email, while in the second, the victim is enticed to a fake website. Malicious attachments or individuals might respond with their data [177].

Many phishing campaigns use maliciously registered domains and sub-domains, leading to substantial financial losses for users worldwide [2]. During the first quarter of 2014, a remarkable 125,215 distinct phishing websites were identified—an increase of more than 11% compared to 2013. Phishing attacks have grown and improved over time, with attackers using more personalized and targeted methods such as spear phishing [80, 22].

2.4.2 Spear Phishing

Spear phishing is an attack designed for specific target systems or users [8]. This attack is intended to compromise highly protected systems effectively. The attackers focus on the weakest link in the security systems, usually the users. Spear phishing targets different users around the world. It is an active attack vector for infiltration into organizations and companies [199]. Spear phishing attacks try to deceive people into giving personal information, installing malware, or unintentionally sending money to the attacker [208]. The attacker may obtain information about the target to make the email look authentic and reliable, such as the email name and address [203, 17]. In addition, messages are designed to

entice the victim, using contextual information and social engineering to fulfill the attacker's target [147]. The target is persuaded to compromise private information using sophisticated attack vectors that appear reliable. These contextual details about the email and victim distinguish spear phishing from regular phishing and strengthen it [60].

Loss from Spear Phishing Attacks

Spear phishing is an attack where the attacker sends fake emails or scripts to targeted individuals or groups of people within the same organization or company [37]. Falling victim to spear phishing attempts may result in numerous adverse outcomes, including financial losses, identity theft, data breaches, an impact on reputation, and cyber espionage. Economic losses result from successful spear phishing attacks, such as stealing money from bank accounts and making illegal purchases. Identity theft, where the attacker steals the identities of individuals or organizations, results in access to sensitive information, including social security numbers, phone numbers, bank cards, and personal data [197, 17]. Data breaches give access to secret information like customer data, trade secrets, and other private data [164, 197]. Spear phishing can damage the reputation of individuals or organizations, particularly if sensitive information is disclosed and the users lose their trust [164, 154, 143].

A Barracuda report discovered approximately 30 million spear-phishing emails after examining 50 billion emails spread across 3.5 million mailboxes. While these emails account for less than 0.1% of all emails sent, they have a significant effect, representing 66% of all attacks on companies [28, 165]. Additionally, IBM reported that the mean cost of a data violation caused by a compromised company email was approximately $4.91 million in 2022 [165]. Facebook and Google were defrauded of $100 million from spear phishing between 2013 and 2015 when phishers issued a series of fake bills to impersonate vendor Quanta [165]. Another study discovered that spear phishing emails are the most common targeted attack, representing approximately 76% of all phishing attempts [187].

Strategies used in spear phishing attacks

Popular spear phishing tactics include personalization, urgency, social engineering, spoofing, and malware [191]. Attackers use personalization to make their spear phishing emails look more credible and trustworthy, such as the victim's name, work title, or other personal information. Urgency is often used in spear-phishing emails to induce victims to respond quickly [31]. Spoofing methods ensure that the received phishing emails are as genuine as possible by using a legal email address or domain name close to a real one. Usually, cybercriminals employ malware to compromise the victims' systems or gain hold of valuable information through malware downloads or links [8]. Spear phishing attempts are likely to be challenging to detect because of their nature [32]. Individuals and organizations can take preventative measures to mitigate the dangers of spear phishing and loss by raising awareness.

2.5 Education and Training

The Security Education, Training, and Awareness (SETA) is an instructional program to minimize security threats resulting from inadequate security consciousness of the workers. In other words, SETA was developed to ensure that the employees understand that they need to pay attention to security issues to prevent themselves, the organization's information, and their network from being compromised. In the SETA program, security is embedded everywhere the employees operate, be it locking the computers when they leave work or reporting strange behaviors involving emails and files [7, 90].

Education and training have been underlined in many studies as the crucial factors that enhance users' awareness and knowledge about spear phishing attacks. The reinforcement of consumers to the long term through education and reminders might help reduce the susceptibility of consumers to spear phishing attacks [163]. Also, it has been established that simulated total features and practice of phishing and spear phishing scenarios are incorporated into the educational applications to enhance the user's resistance to the attacks [44].

2.5.1 Training effect on security

Wombat Security Technologies (2017) observed a significant improvement in users' capacity to identify and report suspicious emails after implementing a training program that included simulated phishing attacks [209]. Similarly, the training programs in individuals and organizations that focused on educating employees about spare phishing attacks resulted in a noticeable decline in successful spear phishing attacks [7].

2.5.2 Training and Education Methods

Companies train users in anti-phishing techniques, including detecting phishing links, using signals to identify phishing, and checking search engines to avoid losses [181, 191]. There are different methods for training users with various success rates that are associated with the users' characteristics. In addition, companies use phishing simulations to send users fake phishing emails to train them to be cautious and detect the features of real phishing emails. Phishing simulations are managed by Chief Information Security Officers, who look at clicked links on emails to assess if the training program is effective. A high number of clicks is considered harmful since this indicates that people failed to recognize the email as phishing, while low click rates are succeeded [149].

In addition, other training depends on game-based, text-based, and video-based methods. Many studies employ game training to teach users engagingly. Games training enables users to interact with tasks to determine if emails are legitimate. Typically, the game incorporates the transmission of information on phishing tactics and identifies phishing emails [192]. In addition, text-based methods use freely available resources, and an instructional book is prepared that includes examples and describes the best strategies for detecting phishing emails. [46, 142]. Video training is utilized in many videos on YouTube for specific purposes. Videos emphasize phishing and offer helpful guidance on recognizing it as well as a fundamental overview of phishing, the tactics employed by cybercriminals, their possible outcomes, and the apparent indications to beware when detecting fraudulent emails and URLs [198].

Education researchers have observed that training is most successful when it includes real examples, tests actual employees, or a testing environment. Several forms of training have been investigated as strategies for reducing phishing [114]. Furthermore, many training methods have examined users' ability to minimize phishing vulnerability. Most training programs contain instructional components to minimize phishing vulnerabilities by educating end-users to recognize and respond to phishing emails [146]. Employees may learn to identify phishing attacks through training programs that update them with the newest threats and trends in spear phishing attacks [191]. However, many studies have found that education did not affect users' knowledge of phishing and legitimate emails [15, 48]. Furthermore, much research supports that in-class education is better for informing users of online training [168, 198].

Despite all these benefits, several limitations mean that people remain vulnerable to phishing attempts for various reasons, such as curiosity about images, which causes 34% of successful attacks [30]. Well-crafted impersonations are email forgeries, unlike the spam that fills the internet, which makes standard email protections ineffective [156]. Furthermore, cybercriminals are constantly developing their strategies [84]. Several academics have also investigated the impact of fear appeal features, which increase the end-user incentive to recognize these emails [68, 104].

2.5.3 Strengths of education and fear appeal approaches

Education strategies are advantageous in several ways. They are instrumental in supporting changes in attitudes and behaviors, and they create a continuous process of change [38]. In addition, depending on the audience characteristics, education strategies can be adapted to increase relevance [91, 158]. Fear appeal strategy assists in modifying attitudes and behaviors; therefore, its significance cannot be overlooked for goal realization. It aligns with audiences driven by fear or threat as they have reduced worry [196].

Education and fear appeal strategies address distinct behavior modification aspects. Education strategies offer information to alter perception and behavior, while fear appeal strate-

gies offer information that precipitates action based on fear or perceived threat [36, 139]. Along with these approaches, the individual, organizations, and governments can develop a sense of urgency while providing the people with the information that will keep the attitude and behavior change going.

2.6 Comparative Analysis

A comprehensive analysis of the efficacy of fear appeals and associated theories determined that fear appeal messages can successfully promote positive changes in attitudes, intentions, and behaviors. However, it is essential to note that there are limited situations in which fear appeals may not be successful depending on factors such as message content, the audience, and the specific context [196]. Fear appeal strategies influence attitudes, intentions, and behaviors. Fear appeal strategies seek to create a sense of fear or threat in the audience to prompt action [196]. Conversely, education strategies impart information and knowledge to modify audience attitudes and behaviors [219].

2.7 Identifying the Research Gap

This study contributes to information security research in spear phishing ground on PMT, and fear appeals [176]. As it stands, there is a research gap that this study aims to fill as it seeks to assess the impact of education and fear appeal approaches to counter spear phishing attacks. Also, A limited experimental study examines awareness of human factors in spear phishing attacks [215]. Also, there is limited research investigating spear phishing attacks on diverse populations [151]. Organizations and individuals need to identify how education and fear appeal interventions affect users' behavior regarding spear phishing because research-based insights can contribute to the strategies of more effective security awareness [176, 191].

2.8 Conclusion

This chapter has identified several key findings about education and fear appeal strategies concerning spear phishing. Training is essential in helping people recognize and report phish-

ing emails and enhance their awareness [117]. In addition, it is noteworthy that the review emphasizes the role of fear appeal about spear phishing attacks [176]. Since phishing is an information security threat, people can still be empowered with the correct information to fight these threats [115]. The literature emphasizes the need for a multi-faceted approach focusing on education, fear appeal messages, and training users to counter spear-phishing threats.

Chapter 3

METHODOLOGY

Spear phishing is a sophisticated social engineering method applied to defraud, obtain sensitive information, or get the intended victims to perform specific actions [9, 122]. The threat of spear phishing attacks is evident and poses a real threat; hence, it constitutes a worrying factor that should be resolved to avert positive attacks [4]. Several prevention measures have been applied in spear phishing studies [50, 94]. This study investigates the efficacy of educational approaches and fear appeal messages and whether the combination of education and fear appeal will work in an experiment to mitigate spear phishing attacks [48, 176].

This chapter provides an overview of the research design, focusing on the method used in this study. The first section addresses the research design, including the research philosophy and quantitative research approach, and how this study adapts the philosophy and approach. The second section illustrates the research strategy and the experiment in this study. The third section defines the target population of end users potentially facing spear phishing risks daily. Section four focuses on data collection and the tools used to collect data. The fifth section describes the data analysis and the software tool used to analyze the data. The sixth section introduces the variables and measures in this study. The seventh section is the ethical consideration in the implementation of this study. The eighth section is the conclusion of the methodology chapter.

3.1 Research Design

3.1.1 Research Philosophy

Positivism is a philosophical perspective grounded in rationalist and empiricist principles [136]. Positivism philosophy strongly emphasizes the value of empirical data and scientific approaches in searching for knowledge. Positivism believes that observable phenomena are legitimate sources of knowledge and uses methodical observation, experimentation, and rational deduction [153]. This philosophy is inclined to measure and transform variables to minimize the researchers' bias in their research [21]. Positivism draws from natural science and philosophy, in which theories are tested against empirical reality to validate or dismiss a theory [152]. Positivism can also be used in social sciences but typically has certain modifications because people and society are not as simple as physical things. This means that, like natural reality, social reality can also be investigated if a worthy approach offers the causes [136]. This philosophy affirms that the study of the social world is uncontaminated by values and is centered on appropriately handling facts [220].

Positivism has been selected as the philosophy in the study due to the predisposition towards accuracy and scientific reliability [12]. Thus, positivism that emphasizes evidence and rational, operative causes might help construct a scientific paradigm. This assists in identifying how education and fear appeal can change the end user against spear phishing attacks [157, 185]. Also, the scientific approach embraced by positivism correlates with the rationale for an empirical evaluation of the efficacy of these interventions [153, 157]. Hence, the positivist philosophy enhances the practical framework for the collection and analysis of data in line with the research aims and objectives.

3.1.2 Research Method

Quantitative research is a scientific inquiry that employs statistical, mathematical, or computational procedures in the empirical collection and analysis of numerical data. This methodology focuses on calculating the data and generalizing the results from a sample to the

target population [21]. For instance, a particular type of research may employ quantitative approaches to assess the rate and intensity of cyber threats in various sectors and to determine the open points and protection methods [124]. Further, it is applied in psychology, economics, and sciences, where numbers give outcomes. The quantitative approach enables the researcher to draw conclusions and forecasts based on the collected data as it is organized and systematically analyzed and interprets data [195].

Rationale for the Chosen Approach

This study employed Quantitative research because I used an experimental method. The experiment examines different aspects and factors relating to spear phishing prevention for end users [5]. In this way, the study supports the results, and the findings are more applicable to the rest of the participants and the end users. This is crucial for drawing meaningful conclusions and recommendations that can be applied [55].

3.2 Research Strategy

The research strategy employed for this study involves using an experimental method to assess participants' knowledge about spear phishing attacks [15]. The experiment design tests the user's knowledge after each intervention to establish cause-and-effect relationships between the interventions and users' knowledge. This study develops the experiment strategy from the literature [74].

3.2.1 Literature review

This study adapts the experiments and questions from instruments already measured in previous literature reviews [15, 93]. The objective of searching the literature is to highlight the pre-existing instruments and metrics for spear phishing attacks to minimize online users' responses. Many studies have used educational intervention to affect users against spear phishing and phishing attacks [74, 191, 200]. Also, many studies used fear to appeal to inform users of attacks, using scenarios and examples to raise awareness about spear phishing

attacks. These scenarios contain various examples of spear phishing attacks, such as fraudulent emails from banks, wrong payments, and compromised Google accounts [94, 101, 176].

3.2.2 Experiments

Each user was assigned randomly to one of these four interventions: education, fear appeal, combined education and fear appeal, and the control group.

Randomized Controlled Trial

This study adopts a randomized controlled trial (RCT). RCT involves allocating participants to the interventions or the control group and is regarded as one of the most helpful research approaches for analyzing the efficacy of an intervention [92, 138]. RCT eliminates bias and examines the connection between an intervention and the outcomes. RCT assists in controlling known and unknown confounding factors within the study populations [189]. This methodology entails randomly assigning the participants into four groups, which would help establish the relationships between the interventions (education, fear appeal, combined) and the measured results [47]. Two previous studies have applied the same approach of educational intervention and fear appeals about phishing [74, 94].

This study combined the benefits of RCT while providing four interventions. This helped test each intervention's efficacy separately and compare it to the other groups. RCT is used in this study due to its benefits, and it has been used previously in other studies with similar areas of interest. To the best of my knowledge, no previous research has used the same study design that I have used here, but many studies have used RCT in their experiments to test phishing attacks.

Education Intervention Group 1:

The first intervention uses education against spear phishing attacks. In education intervention, the material is designed to teach users the indicators of spear phishing attacks to help

them identify this attack [20]. The intervention starts by showing the participants a training video generated in (www.moovly) with duration (00:01:07). The video was created to simulate a training program for spear phishing attacks by explaining the attack definition, how the attacker generates spear phishing emails, the consequence of the attack and the most indicator for these attacks. Also, the participant will see five examples of spear phishing attacks to highlight the most famous examples designed in the Cisco training program [50]. Combining these two educational contents might be beneficial in protecting against spear phishing.

Fear Appeal Intervention Group 2:

In fear appeal, intervention starts by showing the users examples of spear phishing attacks, including the most popular indicators. Then, show the participants a video created on (www.moovly) with duration (00:02:51). The video creates a sense of fear by showing them different spear phishing scenarios and the consequences of these sciences. The video has many senses of danger to manipulate the users' feelings and behaviors about this attack. This video explained common fear appeal scenarios utilized in spear phishing attacks to obtain user reactions and responses. These scenarios detail cybercriminals' strategies to lure victims into completing specific tasks based on their feelings through email [5, 108]. For instance, the first scenario of the email appeared to be from the bank's required response to prevent financial transactions. This scenario relied on the aspect of the loss frame [78]. In the second scenario, the email created urgency by giving the wrong payment information and insisting on immediate action [6]. The third scenario is about a compromised Google account and asking the users to change their passwords as soon as possible [98].

Education and Fear Appeal Intervention Group 3:

This study used a combination of education and fear appeal interventions, offering training on education and fear scenarios to encourage users to apply preventive measures against spear phishing attacks [74]. This intervention includes the same education and fear appeal

videos and examples of education and fear appeal groups. Based on the investigator's understanding of PMT theory, combining these two interventions will cover self-efficacy, response efficacy, threat vulnerability, and threat severity. This might provide a more comprehensive intervention against spear phishing attacks.

Control Intervention Group 4:

A control is a group that does not receive any of the previously stated experimental interventions. The purpose of this group is to provide a baseline for comparison. For the control group, this study used a video named Scenes created by Dr. Marc Dupuis's YouTube channel [66]. The video contains no information about spear phishing attacks or any intervention to protect against them. This video might not affect the participants' behaviors or knowledge regarding spear phishing attacks [99]. The video only contains different senses from nature with time (00:02:06).

After doing the experimental interventions or the control group, the participants answered questions related to the PMT theory to measure the impact of the interventions on the five constructs of the PMT theory.

PMT Constructs:

Protection motivation theory (PMT) is a conceptual framework that explains how persuasive communication influences protective behavior by giving special attention to the cognitive processes involved in fear appeals and behavioral change [130]. This study adopted the questions related to PMT from a survey that tested users' related security behaviors [175]. Schuetz's study developed this instrument to measure the five aspects of PMT: threat severity, vulnerability, response efficiency, self-efficacy, and response cost. Schuetz developed the questions from the previously developed instrument to address how fear impacts users' behavior towards spear phishing attacks. The reliability of the questionnaire was tested using Cronbach's alpha ($\alpha \geq 0.7$). Also, the questionnaire has a convergent validity with

(AVE $\geq$ 0.5), making it suitable [121, 175]. Using a PMT questionnaire, these instruments test spear phishing threats [175].

After the interventions, the participants were presented with the PMT questions. This question tests the spear phishing threat in five aspects: threat severity, vulnerability, response efficacy, self-efficacy, and response cost. Threat severity tests the participants' belief of the danger of spear phishing attacks; threat vulnerability tests the chance that the participants might be a victim of spear phishing attacks; response efficacy tests the participants' response to minimize or prevent spear phishing attacks; self-efficacy tests the participant's efficiency and confidence to identifying a spear phishing attack; and response cost measures the possible cost of flow or not the instructions to mitigate spear phishing attacks [169]. The five aspects were tested by three statements measuring a 7-Likert scale from strongly disagree to strongly agree. The questions adopted from the Schuetz study to measure the PMT for spear phishing attacks [175].

Spear Phishing Test

After the PMT questions, a section tests participants' knowledge of spear phishing attacks. This section measures the participant's knowledge about identifying spear phishing and legitimate emails after the intervention. The spear phishing test includes eight examples of spear phishing and legitimate emails, and in each email, the participant was asked to identify the email as either spear phishing or legitimate emails. Also, the participants were asked to choose the indicators that helped them to indicate the spear phishing attacks using 5- Likert scales starting from strongly disagree to strongly agree [27, 74, 200].

The last section is demographics. The demographics questions ask the participants about their age, gender, and education level. Collecting user information, such as age and gender, will help interpret the results accurately.

3.3 Participants

The population for this study is the end-users, including individuals and employees who use email. This includes all end users irrespective of gender, organizational affiliation, and age above 18 [17]. This may include professionals, students, and people from different parts of society. This study investigates the effectiveness of education and fear appeals against spear phishing to address a broad spectrum of end users most susceptible to spear phishing threats [180]. The experiment requires gathering information from respondents of different ages who may have limited or extensive experience in online security [16, 117, 180]. This population was comprised of different participants to determine the response to education and fear appeal concerning risks because of spear phishing attacks.

3.3.1 Pilot study

Initial review

After reviewing interventions and questions in the experiments, I reviewed the survey questions with people from different backgrounds and majors. The review ensures the questions are understandable to most people.

Pilot study

After reviewing the questions and interventions, a pilot study was conducted to verify the measurement items. Participants joined the survey through Amazon Mechanical Turk [52]. Participants were randomly assigned to complete one of the four experiments administered via the study. Twenty-seven participants were assigned to different experiments. Each experiment contains four quality control questions: "Verifying the legitimacy of an email - for this question, please select disagree." The sentence asks participants to choose "Disagree" to pass the first quality control question. In the second question, "Taking time to verify every email carefully- please select agree," the sentence asks participants to choose "Agree" to pass the second quality control question. Also, the survey has Quality control questions for gender

and ethnicity matching. The participants will receive a control message if they fail to answer any quality control question. This control message is "You have failed one or more quality control questions. The experiment is being ended here instead of a rejection on your record. Please return this task so someone else may complete it. The results you have completed thus far will be discarded." This message explains to the participants that they have failed one or more quality control questions, leading to their experiment response's termination. It also assures them that this termination won't negatively impact their record [67].

After the pilot study, I found that five participants failed the quality control questions. In this pilot study, one participant failed in two quality questions, and one failed in the gender quality question. Also, four participants failed in the first quality questions but not the second. The total number of participants in the pilot study is 21, and five failed participants. The total percentage of rejection rate is 18%.

Sample Size

This study population is end users, including individuals and employees who use email. A large number of the population ensures the accuracy of this study's results.

This study has a 726-sample size for the entire group. All the education and fear appeal groups had the same number of participants, 187 for each group. Moreover, the combined education and fear appeal and control groups had the same sample size, and this was 176.

3.4 Data Collection

3.4.1 Data Collection Instruments

This study developed four experiments to gather data and was launched via an online survey through Qualtrics platforms from May 1 to May 3, 2024. Qualtrics is a cloud-based platform for managing surveys and experiments [137]. It enables users to design and administer surveys to collect information from the target population. Qualtrics is a commonly used tool in academic research, which creates surveys and gathers participant data. The four

experiments enlisted many participants from the Qualtrics platform, which can generate many responses [73]. Qualtrics has features that assisted in developing the survey in this study: To enhance the study's validity, Qualtrics randomly split participants into various experiments. This feature of randomization has made it possible to include hypothesis testing in this study and searches for if there is a connection between the intervention and the result. Further, several aspects of Qualtrics can assist with implementing this research: the four types of experiments, the definition of the logic in questions, the randomization of participants, and the multimedia/images and videos [137].

Several questions were asked in this survey, adopting the Likert scale, to measure the respondents' current level of awareness and practice of spear phishing attacks. Likewise, the Likert scale is a rating scale employed in measuring attitudes, perceptions, opinions, and behavior [193]. These propositions provide a backdrop or context where users can determine their knowledge levels [174].

Data Collection Procedure

This study employed Amazon Mechanical Turk (MTurk) to share the experimental instrument. MTurk remains a convenient and effective work site that allows investigators to gather study data. The platform enables researchers and workers to post-human intelligence tasks (HITs), undertake these tasks, and get paid for them [52, 135]. It is for these reasons that MTurk is very useful. MTurk as a means of collecting data is more efficient and costs less than conventional approaches. Data scientists can recruit different categories of workers who work for pay [62, 106, 141]. It quickly gathers the data. Although it affects the level of participation based on the time taken to receive payment, it does not affect data quality [140]. Previous research has documented that MTurk data is valid and trustworthy and can be as effective as more conventional forms of data gathering in the social sciences. Furthermore, with the help of MTurk, one can invite significant and various numbers of participants, which can be helpful when it is difficult to recruit participants through more conventional procedures [132, 140]. Due to its virtuality, the researcher is not physically with the participant;

this may lead to poor monitoring and compromise data quality [179, 219]. The following scales were used to capture the various objectives of the study. Data quality control measures excluded participants who failed to answer essential questions right to the end of the study [144]. This data collection approach sought to develop viable data that could be used to assess the impact of the interventions implemented on users to detect spear phishing attacks. Each participant received $2 in compensation for completing the survey.

3.4.2 Validation and Reliability Measures

This study used SmartPLS to measure the validity and reliability. It used a SmartPLS because it has many algorithms that help to analyze this study data accurately [167]. This study's reliability has been measured by Cronbach Alpha values and Composite reliability values. The Cronbach Alpha has a minimum threshold value of ($\alpha \geq 0.7$), and the Composite reliability has an (AVE ≥ 0.5) [121]. The Validity was measured using the Heterotrait-Monotrait ratio (HTMT) to measure the correlation between trait correlations and the within-trait correlation between two constructs [216].

3.5 Data Analysis

The Statistical Package for Social Sciences (SPSS) and Smart Partial Least Square (SmartPLS) tests were employed to analyze this study's findings. The first research question was tested using a one-way ANOVA test in SPSS [24]. Regarding the second research question, the SmartPLS algorithm was employed [167]. The data collected in this study is analyzed by SPSS and Smart PLS. SPSS Version 29.0.1.0 has several characteristics and applications to this study, as mentioned below [150]. SPSS has descriptive statistics that enable to analyze and summarize participant information and their perception by demographic data. Therefore, data analysis and an evaluation of the effectiveness of the interventions against spear phishing were done and evaluated in the SPSS for evaluation [24]. The various intervention measures were developed by analyzing the mean of four groups: the education intervention group, the fear appeal intervention group, the combined education-fear appeal intervention

group, and the control group. In this research, the participants were grouped through RCT and assigned randomly to the groups. Applying an ANOVA statistical test can establish whether these groups differ significantly from the control group [57]. In this case, ANOVA helped determine whether such intervention had any significant progress as the means of the four groups were compared.

The following five hypotheses on PMT questions were formulated for this study and tested by the SmartPLS tool. Every PMT factor includes three consistency variables. These hypotheses of this study were tested using the t-test and p-value in comparing each PMT question with the spear phishing test [210]. The first research question addressed these hypotheses and was analyzed using SPSS:

H1: Higher levels of educational intervention have a high effect on users' knowledge for identifying spear phishing attacks compared to the control group.

H2: Higher levels of fear appeal intervention have a high effect on users' knowledge for identifying spear phishing attacks compared to the control group.

H3: Higher levels of a combination of education and fear appeal intervention have a high effect on users' knowledge for identifying spear phishing attacks compared to the control group.

The second research question addresses these hypotheses, and it is analyzed using Smart-PLS:

H4: Higher level of threat severity is associated with higher levels of performance in the spear phishing test.

H5: Higher level of threat vulnerability is associated with higher levels of performance in the spear phishing test.

H6: Higher level of response efficacy is associated with higher levels of performance in the spear phishing test.

H7: Higher level of self-efficacy is associated with higher levels of performance in the spear phishing test.

H8: Lower response cost is associated with higher levels of performance in the spear

phishing test.

3.6 Independent and Dependent Variables

3.6.1 Independent Variables

In this study, the independent variable is the type of intervention or treatment being manipulated. In this case, there are four independent variables:

1. Education intervention: This variable includes providing participants with information and training about spear phishing attacks and preventive measures.

2. Fear Appeal intervention: This variable includes fear appeal messages and scenarios to frighten the participant about spear phishing attacks. It also consists of the potential consequences of falling victim to evoke fear and motivate users to take preventive action.

3. Combination of education and fear appeal intervention: This variable consists of an intervention delivering both educational content and fear appeal messages.

4. Control intervention: This variable did not receive any intervention, so it can help compare this group with other groups that have an intervention.

5. PMT constructs questions that measure the participant's knowledge about spear phishing attacks.

3.6.2 Dependent Variable

The dependent variable will be the outcome or behavior that measures the effect of the independent variables. In this study, the dependent variable is:

1. The result measures the participant's ability to identify spear phishing and legitimate emails in the spear phishing test.

3.7 Ethical Considerations

This study was approved by the Institutional Review Board (IRB) of the University of Washington. Ethical conduct of the research is essential because this research deals with online

security and user behaviors [61]. Firstly, the study gathers all the participants' agreements before they start the survey [105]. Then, the participants' information related to their personality, job, and significance will be secured and not revealed on social media platforms [61]. In addition, the study will be conducted based on volunteering, and participants will be allowed to withdraw at any time without fear of consequences. Also, the experimental instrument is designed to contain no potentially harmful content or trigger language. The learning educational and fear appeal components may remain informative without inflicting undue stress on the target population [212]. Moreover, the result analyzed was conducted ethically. The data obtained were presented anonymously to keep the identity of participants intact [213].

3.8 Conclusion

This chapter describes how the study was conducted and contains information on the experimental design used to reach the study objective. It is intended to provide a detailed description of the experiment and the intervention. This study employed a quantitative research method, specifically experiments. This chapter includes data collection and ethical considerations.

Chapter 4

RESULTS AND DISCUSSIONS

The study contained four groups: education, fear appeal, combined education and fear, and the control group. Each group examined a different intervention, and participants were randomly assigned. Each experiment included a spear phishing test to identify spear phishing and legitimate email phishing and five PMT construct questions. To determine the impact of the intervention on the participants and to test the hypotheses in this study, each intervention group is compared with the control group in the mean score of the spear phishing test. Also, the hypothesis for each PMT construct was evaluated in the spear phishing test for all groups. The demographic characteristics of participants and their performance are included for the four groups. A discussion of the survey questions' results, reliability, and validity is presented, too.

4.1 Study Participants

This study collected data related to participants' demographic data. The data include questions for gender, age, ethnicity, education level, employment status, undergraduate major, work, participant level of formal Computer Science, and the industry currently or most recently worked. Seven hundred twenty-six participants were randomly assigned to the four study groups. Table 4.1 shows the demographic data of all participants. The percentage of male participants exceeded the females by 15.5%. The majority of the study participants were White/Caucasian, with percent 96.6%. Also, 80.9% of the participants had a bachelor's degree.

Table 4.1: Demographic Information

Demographic	**Category**	**Percentage (%)**
Gender	Female	42.1
	Male	57.6
	Non-Binary	0.3
Ethnicity	Asian/Pacific Islander	1.2
	Black/African-American	0.8
	White/Caucasian	96.6
	Hispanic/Latinx	0.6
	Native American/Alaskan Native	0.7
	Other/Multi-Racial	0.1
Age (years)	20-29	35.2
	30-39	44.4
	40-49	10.6
	50-59	7.1
	60-69	2.4
	70-79	0.3
Education	Did not graduate high school (12th grade or less)	0.1
	Graduated high school or equivalent (GED)	1.8
	Some college, no degree	1.2
	Associate degree	2.2
	Bachelor's degree	80.9
	Master's degree	13.4
	Law degree, M.B.A., or other professional degree	0.4
Undergraduate Major	Computer Science	42.4
	Business	31.7
	Engineering	10.5
	Social Science	8.5
	Natural Science	3.0
	Arts and Humanities	2.3
	Other	1.4

This study utilized quality control questions in survey questions to ensure the quality of the answers. Various groups rejected the quality control questions. The quality control questions were as follows:

1-The first question requested the participants to answer "Disagree."

2-The second question requested the participants to answer "Agree."

3-The gender question and ethnicity required the participants to assign their gender and ethnicity at the beginning of the survey and the end and compare their answers.

The quality control questions helped to ensure the participants read the questions instead of answering them randomly without reading [42, 133]. The total rejection rate was 18.73% for the whole participants' pool. After collecting the data, an automated matrix was used to check their accuracy.

Table 4.2: Participants in the main study

Participants	Failed Quality Control						Total
	Q1 only	Q2 only	Gender	Ethnicity	Total Rejection	Rejection rate	
862	103	10	15	8	136	18.73%	726

After the quality control questions, this study has 726 participants for all groups. Table 4.3 shows the number of participants for each group.

Table 4.3: Final Number of participants in each group

Intervention	Participants
Education Intervention	187
Fear Appeal Intervention	187
Combination Educational-Fear Appeal Intervention	176
Control group	176

4.2 Data validity and reliability

4.2.1 Reliability

Reliability describes the internal consistency of variables. When the same result is continually obtained using the same procedures under the same conditions [18]. Reliability is essential in research because it assesses the quality of the findings by verifying their accuracy. It is the degree to which PMT questions produce the same result on repeated trials. This study used SmartPLS to assess the reliability of the survey questions [167]. Reliability was assessed by examining each construct's Cronbach Alpha and Composite reliability values. Cronbach's Alpha measures the internal consistent responses across similar objects [110]. This study assessed the reliability of the PMT questions for all four groups. Reliability was assessed by examining each construct's Cronbach Alpha and Composite reliability values.

Table 4.4: Cronbach Alpha Reliability Test For PMT

Variable	Cronbach's Alpha Value
Threat severity	0.718
Threat vulnerability	0.853
Self-efficacy	0.826
Response efficacy	0.632
Response cost	0.877

The threat vulnerability, self-efficacy, and response cost have values between (0.8 and 0.9), which refers to a good consistency value. Also, an indicator was removed for the threat severity and response efficacy constructs to improve their reliability measures. This helped push the threat severity to construct over the required thresholds with an acceptable value of 0.718. In contrast, the reliability values for response efficacy at 0.632 and 0.634 for Cronbach's Alpha and Composite reliability remain below the 0.700 thresholds. Although the original Cronbach Alpha value was below the threshold value before removing an indicator, the low value of the Composite reliability score warranted its removal. Nonetheless, given their proximity to the threshold and the AVE values (validity) for all constructs above the 0.500 thresholds, this study is okay with these suboptimal values for the response efficacy construct [81].

4.2.2 Validity

Validity refers to how the approach effectively measures what it is intended to measure. It measures how effectively the instrument represents the idea or construct it is designed to measure [110]. This study used SmartPLS to measure the validity of the five PMT constructs and spear phishing test questions. Validity was tested using the Heterotrait-monotrait ratio (HTMT). This study assessed the validity of the PMT and spear phishing test questions for all groups. The HTMT values range was below 0.9, representing a strong correlation and

accurate value [87]. Thus, the questions used were valid.

4.3 Spear Phishing Test Score for Four Groups

This study examines the different interventions related to spear phishing attacks. The study had four groups that had different interventions:

- Participants who joined Group One were affected by educational intervention against spear phishing attacks, which included a video and examples of spear phishing attacks.

- Participants who joined Group Two were affected by a fear appeal intervention, which included a video about the consequences of responding to spear phishing attacks.

- Participants who joined Group Three were affected by combined education and fear appeal Intervention, which included the same content as Group One and Group Two combined.

- Participants who joined Group Four had no effect from spear phishing attacks, which included a video that was a scene from nature.

The participants' knowledge was measured using a spear phishing test with eight examples of spear phishing and legitimate emails. All four groups did the same test with the same questions Figure 4.1 shows the spear phishing test scores for all four groups.

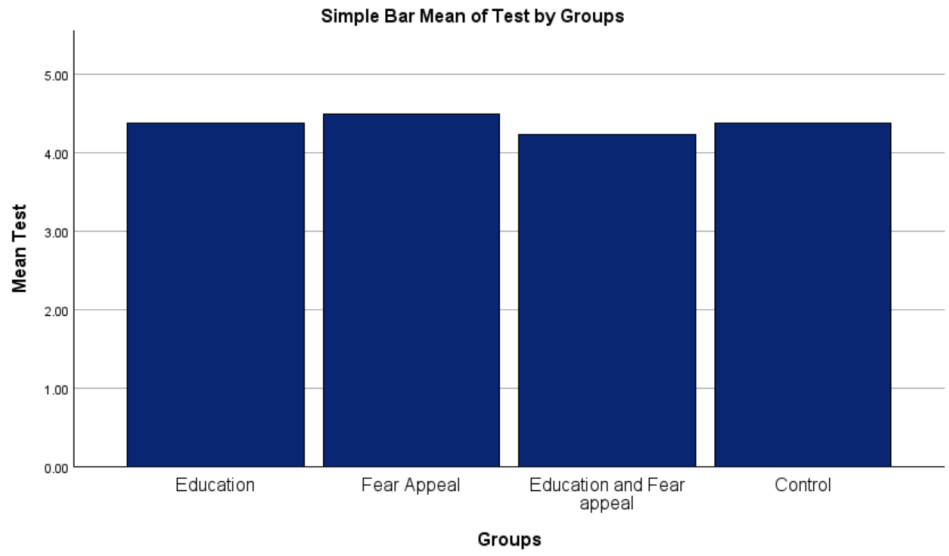


Figure 4.1: The mean Test for four groups

This study compared the scores of the first three groups to the control group. Figure 4.1 shows that all groups had similar spear phishing test scores. SPSS (version 29.0.1.0) was used to measure the difference between the means of the four groups.

This part of the study compared the mean of spear phishing test scores between the education vs. control groups and fear appeals vs. control groups and combined education and fear appeals vs. control groups. The spear phishing test scores of the education, fear appeal, combined education and fear appeal, and control groups all have a normal distribution shape. As a result, this study used a parametric test to measure the data. To measure the performance of participants who joined the (education, fear appeal, combined education and fear appeal) groups and control group, this study used One Way ANOVA [79].

The ANOVA is a statistical measure that is used to measure two or more independent groups to determine if there are any statistically significant differences between them. The ANOVA measures the mean of the spear phishing test scores of each (education, fear appeal, combined education, and fear appeal) group and compares it with the mean of spear phishing test scores of the control group to calculate if there is a significant value between them. If

the result of the significant value in ANOVA is less than (0.05), it indicates that there is a difference between the two groups' scores, but if the value is greater than (0.05), it refers to no significant value across the education and control groups. Also, ANOVA measures Sum Of Squares, Df, Mean Square, and F. The Sum Of Squares is calculated by the squared differences between all the means and each group's mean. Df is the number of independent information available for estimating a statistical parameter. Mean Square is calculated by dividing the Sum of squares by Df. F is the mean square between groups to the mean square within the groups [109].

The same statistical analysis was used to compare the spear phishing test score three times (education vs. control), (fear appeal vs. control), and (education and fear appeal vs. control).

4.3.1 Education Intervention Group vs. Control Group (H1)

To assess the impact of education intervention, a mean score of the group that received an education intervention must be determined and compared with the control group, who did not receive any education intervention. Based on this hypothesis, the participants who underwent the educational intervention should perform better in the spear phishing test than participants in the control group. In testing this hypothesis, the first analysis to be conducted in this study is the test to compare the result of the education group to the control group. The education group consists of 187 participants who participated in only education intervention, while the control group consists of 176 participants. The participants who comprised the education group were between 20 and 80 years old and had varying levels of education and fields of specialization. The participants in the control group were aged between 20 and 65 years and had different education levels and studies majors.

Results:

This study compares the Mean of the education and control groups using a one-way

ANOVA test. The p-value from the ANOVA test is 0.996, greater than 0.05. Thus, this indicates no significant differences between the scores of the education and the control groups. The use of education intervention did not affect the participants' knowledge of identifying spear phishing compared to the control [109].

Table 4.5: ANOVA Test Education and Control

	Sum of Squares	Df	Mean Square	F	Sig
Between Groups	.000	1	.000	.000	.996
Within Groups	559.047	361	1.549		
Total	559.047	362			

Discussion:

The first aim results show no significant impact of the education intervention on enhancing the participants' spear phishing knowledge compared to the control group, which contradicts the first hypothesis. From this result, it is evident that the findings support the null hypothesis, which posits that educating participants on spear phishing does not help them improve their awareness of spear phishing attacks. On average, the means obtained for both experiments are almost the same. This might indicate that the education intervention did not realize the knowledge gained among participants needed to identify spear phishing effectively.

There might be different reasons why educational intervention impact varies from one study to another, mainly due to the variability in the content, education time, and duration [15]. In contrast to previous studies that have shown that education intervention enhances cybersecurity awareness and knowledge [131, 163]. This study finding aligns with some studies that indicate insignificant outcomes of educating users about phishing attacks [15, 48, 198].

Alghamdi's (2017) study found that educating users using examples and text-based is

ineffective for identifying phishing attacks [15]. Also, Caputo et al.(2014) explain how online training is inadequate as many users have not read the training [48]. In addition, Tschakert and Ngamsuriyaroj's study supports users who prefer in-class training [198].

This study sought out to determine the efficacy of education in helping users better detect spear phishing emails. The study results suggest that there may be better methods for helping individuals become better equipped to deal with spear phishing emails. For example, Jampen et al. (2020) discovered that training post-attack users is a better practice than conventional training [99]. According to Sheng and Hong (2007), the method of phishing simulation training would help users improve their awareness of the attack. Further, the simulation enables the users to make decisions toward identifying phishing attacks [181]. Moreover, Xiong et al. (2019) also noted that embedded training has made users more conscious of phishing attacks [214]. Therefore, more future research needs to use classroom and embedded training instead of online test-based and short videos [198].

4.3.2 Fear Appeal Intervention vs. Control Group (H2)

To determine the intervention effect of the fear appeal, this study measured the score of the group with fear appeal intervention against the score of the groups with no intervention, the control groups. According to this hypothesis, the participants who have been through the fear appeal intervention could have scored higher on the spear phishing test than those who joined the control group. To test this hypothesis, this study will begin the first analysis by comparing the participants' performance in the fear appeal group with those of the control group. The fear appeal group consists of 187 participants who participated in only fear appeal intervention, while the control group consists of 176 participants. The participants who joined the fear appeal were 20 to 70 years of age, had varying education levels, and had majored in different fields. The control group members included participants ranging in age from 20 to 65; they had different education levels and majors.

Results:

Using a one-way ANOVA test, this study compares the Mean of two groups: fear appeal

and control. The p-value from the ANOVA test is 0.398, more significant than 0.05. This indicates no significant differences between fear appeal and the control groups in spear phishing test scores. This suggests no significant effect exists between fear appeal intervention and the control group. The use of fear appeal intervention did not affect the participant's knowledge of identifying spear phishing attacks. Table 4.6 shows the result of the ANOVA test [109].

Table 4.6: ANOVA Test Fear Appeal and Control

	Sum of Squares	Df	Mean Square	F	Sig
Between Groups	1.294	1	1.294	.715	.398
Within Groups	651.745	360	1.810		
Total	653.039	361			

Discussion:

The second aim shows no significant effect of fear appeal interventions on improving the participants' knowledge compared to the control group, which is inconsistent with the second hypothesis and supports the null hypothesis. The null hypothesis indicates that the appeal of fear does not affect users' knowledge of identifying spear phishing attacks. The mean results for both groups are similar. This resulted in the fear appeal intervention not having a significant effect on identifying spear phishing attacks.

Many studies have found that a high level of fear appeal does not significantly affect the user's knowledge [100, 119]. However, these results are controversial to many researchers who have proven that fear appeal could improve users' responses to phishing attacks [196, 101].

Lawson et al. (2016) study found that exposing the participants to fear appeals on docudrama videos without explicit and proper instruction leads to hopelessness and confusion among participants [119]. Moreover, two research correspond to this study, which shows that intense fear of video can sometimes lead to adverse actions, which may affect the participants'

behaviors by causing them to delete or avoid their emails [100, 161]. Furthermore, this study utilized a video with a fear appeal message only once, which, according to Shi and Smith (2016), probably was ineffective in identifying spear phishing attacks [182]. Even though the people in the fear appeal intervention group in this research have the highest scores on the test against other groups, this difference was insignificant statistically compared to the control group. This implies that even though fear appeal interventions may help enhance the participant's level of knowledge, they would not improve their test results on spear phishing attacks.

This study sought to determine the efficacy of fear appeal in helping users better detect spear phishing emails. The study results suggest that there may be better methods for helping individuals become better equipped to deal with spear phishing emails. Many studies argue that fear text should be used based on users' behaviors [101, 102]. Also, Burita et al. (2022) support the actual simulation of sending users phishing emails to measure if the users click the phishing links [44, 94]. Furthermore, Tannenbaum et al.(2015) support using fear appeal messages to change the user's attention and behaviors [196]. Therefore, future research should develop a text-based message for the fear appeal intervention rather than the video.

4.3.3 Combined Education and Fear Appeal Intervention vs. Control Group (H3)

To determine the impact of both the education and the fear appeal interventions, this study requires the score of the control group and the third group that has received both the education and the fear appeal interventions. According to hypothesis three, it was expected that the participants who received both the educational and the fear appeals intervention would have higher test scores than those in the control group. To test the validity of this hypothesis, the following study compared the Spear Phishing Test score of the education and fear appeal group to the control group. The combined education and fear appeal group targeted the following participants: 176. Also, there were 176 participants in the control group, which equals the number of participants in both groups. People in the combined education and

fear appeal group were of different education, ages ranging from 20 to 70. Participants from the control group were also selected from different educational backgrounds, aged between 20 and 65.

Result:

This study compares the mean of two groups, combined education and fear appeal interventions, to the control group, using a one-way ANOVA test. The p-value result from the ANOVA test is 0.297, which is greater than 0.05. This indicates that there are no significant differences between the spear phishing test scores of the combined education and fear appeal and the control groups. This indicates that the combined education and fear appeal had no significant effect on the participant's knowledge of identifying spear phishing compared to the control. Table 4.7 shows the result of the ANOVA test [109].

Table 4.7: ANOVA Test Educational-Fear Appeal and Control

	Sum of Squares	Df	Mean Square	F	Sig
Between Groups	1.776	1	1.776	1.089	.297
Within Groups	570.699	350	1.631		
Total	572.474	351			

Discussion:

The study's third aim shows no significant effect of combining education and fear appeal intervention of spear phishing test scores compared to the control group. This result was inconsistent with the third hypothesis, which assumes that having a combined education and fear appeal affects users' knowledge of identifying spear phishing attacks compared to the control group. This result supports the null hypothesis, indicating that the combination intervention has no significant effect compared to the control group. However, Zielinska et al. (2014) study found that education training that includes fear training can enhance the user's knowledge of identifying phishing attacks [218].

The result supports the null hypothesis, which indicates that a combination of online education and fear appeal does not affect the participants' performance in identifying spear phishing attacks. The non-significant findings suggest that the combination of education and fear appeal intervention has not significantly enhanced the participants' ability to recognize spear phishing emails. Several studies measured education and fear appeal as separate factors and explained that they do not affect the participant's behavior [15, 119, 198]. Therefore, the study findings indicate insufficient evidence to support that the combination of education and fear appeal produces no effect on the participants' knowledge level and capability to identify spear phishing emails.

4.3.4 PMT Hypotheses

Results:

This study examines the different PMT factors related to the test of spear phishing attacks. The study has five aspects of the PMT construct (threat severity, threat vulnerability, response efficacy, self-efficacy, and response cost). Due to the lack of statistically significant differences among the different experimental groups, all were combined into a single group for analysis purposes to assess the PMT model. This study will measure the effect of five PMT constructs on the spear phishing test. This study used SmartPLS to calculate the t-test and p-value for the spear phishing test of all groups. It used a t-test to measure if there was any significance in the mean between the groups. Also, the p-value is used to find the relationship between two constructs [184]. Also, the study calculated the R-Square to measure the dependent variable's variance explained by independent variables [69]. Table 4.8 shows how PMT construction affects the test result. Also, Figure 4.2 shows the effect of PMT on the Spear phishing test.

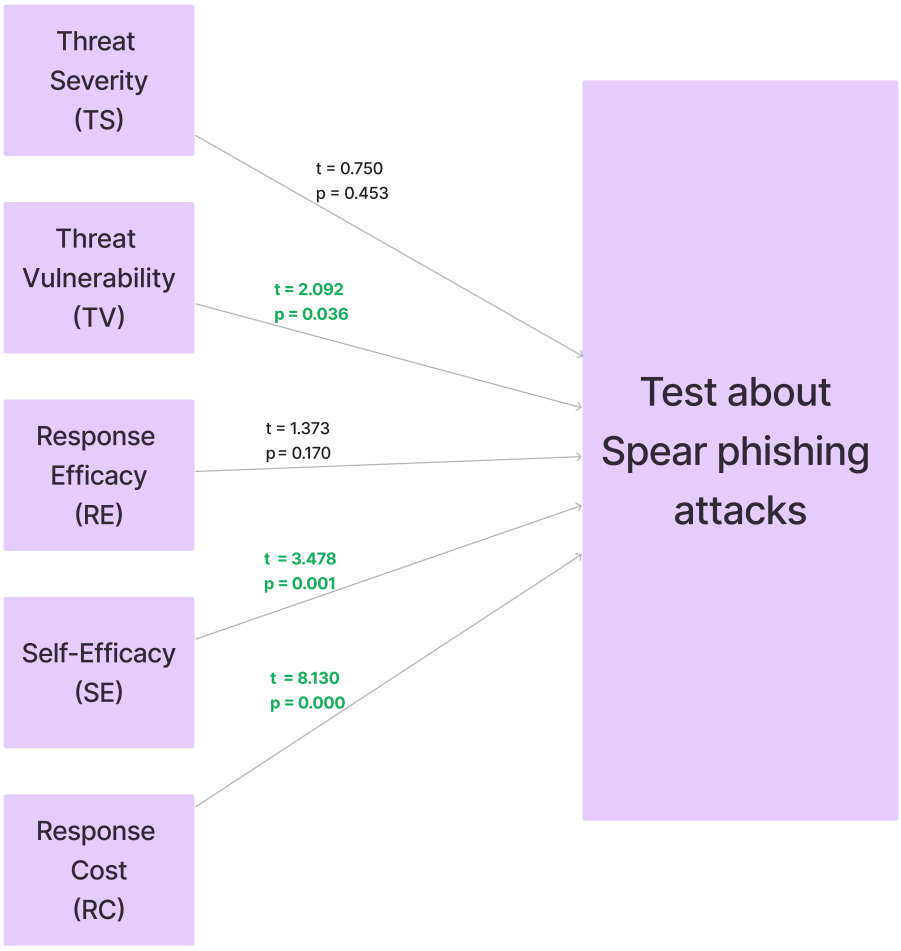


Figure 4.2: The Effect of PMT on Spear phishing test result

Table 4.8: Summary of Statistical Tests

PMT Constructs	T statistic	P-value	Supported?
Threat Severity: H4	0.750	0.453	Not Supported
Threat Vulnerability: H5	2.092	0.036	Supported
Response efficacy: H6	1.373	0.170	Not Supported
Self-efficacy: H7	3.478	0.001	Supported
Response cost: H8	8.130	0.000	Supported
$R^2 = 30.4\%$			

This study measures the effect of the five PMT constructs on participants' knowledge regarding spear phishing tests. Table 4.8 shows the t-test and the p-value of the five PMT constructs in relation to the result. The p-value of these relationships measured the significance of the effect of PMT constructs on the spear phishing test. If the p-value is less than 0.05, it indicates a significant impact, supporting this study's hypothesis. Depending on the p-value, this study supports three PMTs (Threat vulnerability, Self-efficacy, and Response cost) that have a statistically significant effect, which had a p-value less than 0.05. Threat vulnerability, Self-efficacy, and Response cost have a statistically significant value in the spear phishing test score, which means that these three factors enhance the participant's knowledge regarding spear phishing attacks.

Discussion:

The fourth aim of this study supports three significant results: a high level of threat vulnerability and self-efficacy enhance users' knowledge about spear phishing attacks. Also, low levels of response costs have a positive effect on improving users' knowledge about spear phishing attacks.

This study supports the positive effect of self-efficacy on participants' knowledge for identifying spear phishing attacks. This result aligns with many studies in the literature, which indicate that Self-efficacy had a significant effect on participants' behaviors in preventing

phishing security [23, 70, 194]. A meta-analysis of 59 studies supports self-efficacy in users' behaviors to take protective action to protect their information security against the threat [83]. However, Lee et al.(2023) found that a high level of self-efficacy has a negative effect on users' attitudes toward sharing their information online [120]. Previous studies show that for users who are overconfident in their ability to identify phishing attacks, it is hard to be convinced about the severe threat of this attack [102]. Also, William and Joinson(2020) found no relationship between self-efficacy and identifying phishing emails [206]. Thus, future studies should not depend on the self-efficacy constructs alone to find spear phishing attacks.

Also, this study supports the positive effect of the low response cost on the participant's knowledge of identifying spear phishing attacks by having a substantial statistically significant value of 0.000. This result supports the current evidence about the benefit of low response cost. According to many studies, the low-cost response makes the users willing to adopt protective action in security behaviors and the users prefer to take action if the cost response is low and acceptable [35, 86, 205, 130]. All the previous studies support that the low cost makes the users more adaptable to take preventive action, which indicates the use of low cost in security training to enhance the users' ability to take protective actions. However, there is a limited study that supports the users are willing to take an action that has a high cost. This might help design future spear training by providing users with a protective action that has a low cost.

Chapter 5

CONCLUSION

This study aims to assess the role of education and fear appeals as protective factors towards spear phishing prevention among online users. The study findings highlight a general overview of the effects of the three intervention groups on spear phishing threats. This means that the study, which had education and fear appeal, did not affect the participants' level of susceptibility to spear phishing attacks. However, the study recognizes that these results could have been constrained by factors like using an intervention's content or the participant's background.

Furthermore, concerning the method of this study, four experiments were conducted in which participants were assigned randomly into four groups. There were three experimental interventions and one control intervention group. The objective is to assess the participants involved in education, fear appeals, and both education and fear appeal interviews by calculating the Mean of their spear phishing test against the two control groups. The results show no significant difference between the groups in the spear phishing test. Further, in this study, the five PMT constructs on the spear phishing test make it evident that self-efficacy threat vulnerability and response cost positively influence the users' knowledge of spear phishing attacks.

5.1 Limitation and Future Work

Limitations are associated with participants' race and education level, survey time, and other factors.

5.1.1 Survey Time

The survey time is different from one group to another, as the third group has more time than the other groups. This is because the third group has two interventions. The average time for the four groups was about 17 minutes. The number of participants also varied in the four groups, as each of the education and fear appeal had 187 participants, and the combination of education and fear appeal and the control group had 176 participants [41].

5.1.2 Participant Background

There are many other factors, such as whether the participants have been exposed to spear phishing attacks or had attended training on social engineering hacks. Also, the participants might inspect their email before responding. In addition, other factors related to participants' awareness and demographics include not sharing personal information [123].

5.1.3 Method of study

This study used an experiment with a single post-test. Many researchers use two tests, pre-tests and post-tests, to measure the effect accurately. Also, this study utilized only image and video [74, 198].

5.1.4 Spear phishing test

The spear phishing test is in a control condition. In the spear phishing test, participants were fully focused on the task. The control test might not reflect the real-world situation when the users received spear phishing emails [172, 116].

5.2 Future work

There are many future directions for this study.

5.2.1 Qualitative Research Method

This study can be designed using a qualitative research method. This method can provide more in-depth detail about human feelings when they receive a spear phishing email [64].

5.2.2 Different Intervention Content

In addition, look into different Interventions methods, for instance, the financial or reputational consequences of a successful phishing attack, to find out which strategy is the most effective for preventing spear phishing [218].

5.2.3 Designed for Specific Demographic

Moreover, studies on specific demographics, such as older people or those with limited technical abilities, should be conducted to develop targeted interventions that meet the needs and vulnerabilities of these groups[123].

BIBLIOGRAPHY

[1] Crowdstrike, 2023.

[2] Earl Andrea Abad, John Rafael Ferrer, and Prospero Naval. *Phishing Website Classification using Features of Web Addresses and Web Pages*. February 2020.

[3] Mumtaz Abdul Hameed and Nalin Asanka Gamagedara Arachchilage. On the Impact of Perceived Vulnerability in the Adoption of Information Systems Security Innovations. *International Journal of Computer Network and Information Security*, 11(4):9–18, April 2019.

[4] Ahmad Syukri Abdullah and Masnizah Mohd. Spear Phishing Simulation in Critical Sector: Telecommunication and Defense Sub-sector. In *2019 International Conference on Cybersecurity (ICoCSec)*, pages 26–31, September 2019.

[5] Hossein Abroshan, Jan Devos, Geert Poels, and Eric Laermans. COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic. *IEEE Access*, 9:121916–121929, 2021. Conference Name: IEEE Access.

[6] Suman Acharya and Sujata Joshi. IMPACT OF CYBER-ATTACKS ON BANKING INSTITUTIONS IN INDIA: A STUDY OF SAFETY MECHANISMS AND PREVENTIVE MEASURES. 2020.

[7] Melad Mohamed Al-Daeef, Nurlida Basir, and Madihah Mohd Saudi. Security Awareness Training: A Review. 2017.

[8] Yuosuf Al-Hamar, Hoshang Kolivand, Mostafa Tajdini, Tanzila Saba, and Varatharajan Ramachandran. Enterprise Credential Spear-phishing attack detection. *Computers & Electrical Engineering*, 94:107363, September 2021.

[9] Abeer F AL-Otaibi and Emad S Alsuwat. A STUDY ON SOCIAL ENGINEERING ATTACKS: PHISHING ATTACK. 2020.

[10] Mahmoud Al-Shawabkeh, Madihah Mohd Saudi, and Najwa Hayaati Mohd Alwi. Computer security self-efficacy effect: An extention of Technology-to-Performance chain model. In *2012 IEEE Control and System Graduate Research Colloquium*, pages 64–69, July 2012.

[11] Rana Alabdan. Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, 12(10):168, September 2020.

[12] Kizito Ogedi Alakwe. Positivism and Knowledge Inquiry: From Scientific Method to Media and Communication Research. 2017.

[13] Hussain Aldawood and Geoff Skinner. *Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review*. December 2018.

[14] Hussain Aldawood and Geoffrey Skinner. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet*, 11(3):73, March 2019. Number: 3 Publisher: Multidisciplinary Digital Publishing Institute.

[15] Hanaa Alghamdi. *Can Phishing Education Enable Users To Recognize Phishing Attacks?*. PhD thesis, [object Object], 2017.

[16] Mohamad Alhaddad, Masnizah Mohd, Faizan Qamar, and Mohsin Imam. Study of Student Personality Trait on Spear-Phishing Susceptibility Behavior. *International Journal of Advanced Computer Science and Applications*, 14(5), 2023.

[17] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, 3, 2021.

[18] DUANE F. ALWIN and JON A. KROSNICK. The Reliability of Survey Attitude Measurement: The Influence of Question and Respondent Attributes. *Sociological Methods & Research*, 20(1):139–181, August 1991. Publisher: SAGE Publications Inc.

[19] Catherine L. Anderson and Ritu Agarwal. Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, 34(3):613–643, 2010. Publisher: Management Information Systems Research Center, University of Minnesota.

[20] Giddeon Njamngang Angafor, Iryna Yevseyeva, and Leandros Maglaras. Securing the remote office: reducing cyber risks to remote working through regular security awareness education campaigns. *International Journal of Information Security*, January 2024.

[21] Stephen Kwadwo Antwi and Kasim Hamza. Qualitative and Quantitative Research Paradigms in Business Research: A Philosophical Reflection. *European Journal of Business and Management*, 2015.

[22] APWG. Anti-Phishing Working Group (APWG) (2014) Phishing activity trends report—fourth quarter 2013. http://antiphishing.org/ reports/apwgtrendsreportq42013.pdf. Accessed Sept 2014. Technical report, September 2014.

[23] Nalin Asanka Gamagedara Arachchilage and Mumtaz Abdul Hameed. Integrating self-efficacy into a gamified approach to thwart phishing attacks, June 2017. arXiv:1706.07748 [cs].

[24] Daniel Arkkelin. Using SPSS to Understand Research and Data Analysis. 2014.

[25] Ayesha Arshad, Attique Ur Rehman, Sabeen Javaid, Tahir Muhammad Ali, Javed Anjum Sheikh, and Muhammad Azeem. A Systematic Literature Review on Phishing and Anti-Phishing Techniques. 2021.

[26] Maria Bada, Angela M Sasse, and Jason R C Nurse. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? 2019.

[27] David S Barnes. *A DEFENSE-IN-DEPTH APPROACH TO PHISHING*. PhD thesis, 2006.

[28] Market Barracuda. 2023 spear-phishing trends. *May,2023*, May 2023.

[29] Samantha Bax, Tanya McGill, and Val Hobbs. Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs. *Computers & Security*, 106:102278, July 2021.

[30] Zinaida Benenson, Freya Gassmann, and Robert Landwirth. Exploiting curiosity and context:.

[31] Debalina Bera, Obi Ogbanufe, and Dan J. Kim. Towards a thematic dimensional framework of online fraud: An exploration of fraudulent email attack tactics and intentions. *Decision Support Systems*, 171:113977, August 2023.

[32] Aniket Bhadane and Sunil B. Mane. Detecting lateral spear phishing attacks in organisations. *IET Information Security*, 13(2):133–140, 2019. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1049/iet-ifs.2018.5090.

[33] Chandra Sekhar Bhusal. Systematic Review on Social Engineering: Hacking by Manipulating Humans. *Journal of Information Security*, 12(1):104–114, December 2020. Number: 1 Publisher: Scientific Research Publishing.

[34] Elisabeth Bigsby and Dolores Albarracín. Self- and Response Efficacy Information in Fear Appeals: A Meta-Analysis. *Journal of Communication*, 72(2):241–263, April 2022.

[35] John M. Blythe and Lynne Coventry. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, 87:87–97, October 2018.

[36] Lynne M. Borden, Sun-A Lee, Joyce Serido, and Dawn Collins. Changing College Students' Financial Knowledge, Attitudes, and Behavior through Seminar Participation. *Journal of Family and Economic Issues*, 29(1):23–40, March 2008.

[37] Johan Brandqvist and John Lieberth Nilsson. Phishing Detection Challenges for Private and Organizational Users: A Comparative Study. page 60, 2023.

[38] Mirjam Braßler and Sandra Sprenger. Fostering Sustainability Knowledge, Attitudes, and Behaviours through a Tutor-Supported Interdisciplinary Course in Education for Sustainable Development. *Sustainability*, 13(6):3494, March 2021.

[39] Filipe Breda, Hugo Barbosa, and Telmo Morais. SOCIAL ENGINEERING AND CYBER SECURITY. pages 4204–4211, Valencia, Spain, March 2017.

[40] Robert Broberg and Philip Sinnott. The Human Element of Cybersecurity: A Literature Review of Social Engineering Attacks and Countermeasures. 2023.

[41] Marc Brysbaert. How Many Participants Do We Have to Include in Properly Powered Experiments? A Tutorial of Power Analysis with Reference Tables. *Journal of Cognition*, 2(1):16, 2019.

[42] Michael Buhrmester, Tracy Kwang, and Samuel D. Gosling. Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data? *Perspectives on Psychological Science*, 6(1):3–5, 2011. Publisher: Sage Publications, Inc.

[43] Linh Bui, Barbara Mullan, and Kirsten McCaffery. Protection motivation theory and physical activity in the general Population: A systematic literature review. *Psychology, Health & Medicine*, 18(5):522–542, October 2013. Publisher: Taylor & Francis _eprint: https://doi.org/10.1080/13548506.2012.749354.

[44] Ladislav Burita, Ivo Klaban, and Tomas Racil. Education and Training Against Threat of Phishing Emails. *International Conference on Cyber Warfare and Security*, 17(1):7–18, March 2022.

[45] A. J. Burns, M. Eric Johnson, and Deanna D. Caputo. Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce*, 29(1):24–39, January 2019.

[46] Gamze Canova, Melanie Volkamer, Clemens Bergmann, Roland Borza, Benjamin Reinheimer, Simon Stockhardt, and Ralf Tenberg. Learn to Spot Phishing URLs with the Android NoPhish App. In Matt Bishop, Natalia Miloslavskaya, and Marianthi Theocharidou, editors, *Information Security Education Across the Curriculum*, IFIP Advances in Information and Communication Technology, pages 87–100, Cham, 2015. Springer International Publishing.

[47] Bernadette Capili. A Primer to the Randomized Controlled Trial. *The American journal of nursing*, 123(3):47–51, March 2023.

[48] Deanna D. Caputo, Shari Lawrence Pfleeger, Jesse D. Freeman, and M. Eric Johnson. Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security & Privacy*, 12(1):28–38, January 2014. Conference Name: IEEE Security & Privacy.

[49] Mei-Fang Chen. Impact of fear appeals on pro-environmental behavior and crucial determinants. *International Journal of Advertising*, 35(1):74–92, January 2016. Publisher: Routledge.

[50] Cisco. What Is Spear Phishing?, 2024.

[51] Marlon Clarke. *The Role of Self-Efficacy in Computer Security Behavior: Developing the Construct of Computer Security Self-Efficacy (CSSE)*. PhD thesis, 2010.

[52] Cihan Cobanoglu, Muhittin Cavusoglu, and Gozde Turktarhan. A beginner's guide and best practices for using crowdsourcing platforms for survey research: The case of Amazon Mechanical Turk (MTurk). *Journal of Global Business Insights*, 6(1):92–97, March 2021.

[53] Mark Conner, editor. *Predicting health behaviour: research and practice with social cognition models*. Open Univ. Press, Maidenhead, 2. ed., repr edition, 2009.

[54] Mark Conner and Paul Norman. *Predicting and Changing Health Behaviour: Research and Practice with Social Cognition Models*. McGraw-Hill Education (UK), May 2015. Google-Books-ID: pMkvEAAAQBAJ.

[55] ThomasD Cook and Donald T Campbell. Trru UNIvERSITYop MEvPrrts. 2002.

[56] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse. Defining Cybersecurity. *Technology Innovation Management Review*, 2014.

[57] Antonio Cuevas, Manuel Febrero, and Ricardo Fraiman. An anova test for functional data. *Computational Statistics & Data Analysis*, 47(1):111–122, August 2004.

[58] John D'Arcy, Tejaswini Herath, and Mindy K. Shoss. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, 31(2):285–318, 2014. Publisher: Taylor & Francis, Ltd.

[59] Aday Destici. DETERMINING THE FACTORS THAT INFLUENCE THE USE OF PRIVACY CONFIGURATION SETTINGS ON FACEBOOK AN EMPIRICAL STUDY AMONG ADOLESCENTS. 2015.

[60] Prateek Dewan, Anand Kashyap, and Ponnurangam Kumaraguru. Analyzing social and stylometric features to identify spear phishing emails. In *2014 APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–13, September 2014. ISSN: 2159-1245.

[61] Lubna Luxmi Dhirani, Noorain Mukhtiar, Bhawani Shankar Chowdhry, and Thomas Newe. Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. *Sensors*, 23(3):1151, January 2023.

[62] Djellel Difallah, Elena Filatova, and Panos Ipeirotis. Demographics and Dynamics of Mechanical Turk Workers. In *Proceedings of the Eleventh ACM International Conference on Web Search and Data Mining*, pages 135–143, Marina Del Rey CA USA, February 2018. ACM.

[63] James Price Dillard, Courtney A. Plotnick, Linda C. Godbold, Vicki S. Freimuth, and Timothy Edgar. The Multiple Affective Outcomes of AIDS PSAS: Fear Appeals Do More Than Scare People. *Communication research, 23(1), 44-72.*, 1996.

[64] Verena Distler. 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*, pages 1–18, Hamburg Germany, April 2023. ACM.

[65] Paul Dolan, Michael Hallsworth, David Halpern, Dominic King, and Ivo Vlaev. MINDSPACE Influencing behaviour through public policy. *Institute for Government, Cabinet Office,*, 2010.

[66] Marc Dupuis, Anna Jennings, and Karen Renaud. Scaring People is Not Enough: An Examination of Fear Appeals within the Context of Promoting Good Password

Hygiene. In *Proceedings of the 22st Annual Conference on Information Technology Education*, pages 35–40, SnowBird UT USA, October 2021. ACM.

[67] Marc J Dupuis. The Role of Trait Affect in the Information Security Behavior of Home Users. 2014.

[68] Nico Ebert, Kurt A. Ackermann, and Angela Bearth. When information security depends on font size: how the saliency of warnings affects protection behavior. *Journal of Risk Research*, 26(3):233–255, March 2023.

[69] Lloyd J. Edwards, Keith E. Muller, Russell D. Wolfinger, Bahjat F. Qaqish, and Oliver Schabenberger. An R2 statistic for fixed effects in the linear mixed model. *Statistics in Medicine*, 27(29):6137–6157, 2008. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/sim.3429.

[70] Danielle Ehizibue. Investigation of Individuals' Behavior towards Phishing Attacks. 2022.

[71] Roghayeh Ezati Rad, Shokrollah Mohseni, Hesamaddin Kamalzadeh Takhti, Mehdi Hassani Azad, Nahid Shahabi, Teamur Aghamolaei, and Fatemeh Norozian. Application of the protection motivation theory for predicting COVID-19 preventive behaviors in Hormozgan, Iran: a cross-sectional study. *BMC Public Health*, 21(1):466, March 2021.

[72] Tom Field. EMAIL SECURITY: SOCIAL ENGINEERING REPORT. Technical report, 2016.

[73] Kathryn Fletcher. Developing Best Practices for Qualtrics Administration. In *Proceedings of the 2016 ACM SIGUCCS Annual Conference*, pages 89–94, Denver Colorado USA, November 2016. ACM.

[74] Sebastian Floderus and Linus Rosenholm. An educational experiment in discovering spear phishing attacks. 2019.

[75] Sebastian Floderus and Linus Rosenholm. An educational experiment in discovering spear phishing attacks. 2019.

[76] Donna L. Floyd, Steven Prentice-Dunn, and Ronald W. Rogers. A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, 30(2):407–429, 2000. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1559-1816.2000.tb02323.x.

[77] Walter Fuertes, Diana Arévalo, Joyce Denisse Castro, Mario Ron, Carlos Andrés Estrada, Roberto Andrade, Felix Fernández Peña, and Eduardo Benavides. Impact of Social Engineering Attacks: A Literature Review. In Álvaro Fuertes, Carlos Hernan Fajardo-Toro, and José María Riola Rodríguez, editors, *Developments and Advances in Defense and Security*, volume 255, pages 25–35. Springer Singapore, Singapore, 2022. Series Title: Smart Innovation, Systems and Technologies.

[78] Athanasia Gianniki. Postgraduate Dissertation "E-banking alongside the increasing number of e-frauds in the post- coronavirus era. Which measures would be more effective in diminishing the problem?". 2023.

[79] Victor Grech and Neville Calleja. WASP (Write a Scientific Paper): Parametric vs. non-parametric tests. *Early Human Development*, 123:48–49, August 2018.

[80] B. Gupta, Aakanksha Tewari, Ankit Jain, and Dharma Agrawal. Fighting against phishing attacks: state of the art and future challenges. *Neural Computing & Applications*, 28(12):3629–3654, December 2017. Publisher: Springer Nature.

[81] Joseph Hair, William Black, and Barry Babin. *Multivariate data analysis (7th ed.)*. Upper Saddle River, NJ: Prentice Hall., 2010.

[82] Tzipora Halevi, Nasir Memon, and Oded Nov. Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. *SSRN Electronic Journal*, January 2015.

[83] Mumtaz Abdul Hameed and Nalin Asanka Gamagedara Arachchilage. The role of self-efficacy on the adoption of information systems security innovations: a meta-analysis assessment. *Personal and Ubiquitous Computing*, 25(5):911–925, October 2021.

[84] Julian Hazell. Large Language Models Can Be Used To Effectively Scale Spear Phishing Campaigns. May 2023.

[85] Ryan Heartfield and George Loukas. A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys*, 48(3):1–39, February 2016.

[86] Sadegh Hedayati, Hossein Damghanian, Mohsen Farhadinejad, and Abbas Ali Rastgar. Meta-analysis on application of Protection Motivation Theory in preventive behaviors against COVID-19. *International Journal of Disaster Risk Reduction*, page 103758, June 2023.

[87] Jörg Henseler, Christian M. Ringle, and Marko Sarstedt. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1):115–135, January 2015.

[88] Diane Henshel, Char Sample, M.G. Cains, and Blaine Hoffman. Integrating Cultural Factors into Human Factors Framework and Ontology for Cyber Attackers. pages 123–137. January 2016.

[89] C Herbert and Jr Peluzzo. *Protecting a New Jersey School District from Cyber Threats: The Role of Cybersecurity Awareness, Training, and Professional Development for K-12 Leaders, Educators, and Staff Members*. Doctoral dissertation, Rider University, 2022.

[90] Stephanie D Hight. The importance of a security, education, training and awareness program (November 2005). 2005.

[91] Bryn Holmes and John Gardner. *E-Learning: Concepts and Practice*. SAGE, June 2006. Google-Books-ID: XbbM9mj22KQC.

[92] Sherilyn Houle. An Introduction to the Fundamentals of Randomized Controlled Trials in Pharmacy Research. *The Canadian Journal of Hospital Pharmacy*, 68(1):28–32, 2015.

[93] DEANNA HOUSE. *An assessment of user response to phishing attacks: The effects of fear and self-confidence.* PhD thesis, 2013.

[94] Deanna House. AN ASSESSMENT OF USER RESPONSE TO PHISHING ATTACKS: THE EFFECTS OF FEAR AND SELF-CONFIDENCE. 2019.

[95] Deanna House and M. K. Raja. Phishing: message appraisal and the exploration of fear and self-confidence. *Behaviour & Information Technology*, 39(11):1204–1224, November 2019.

[96] Deanna House and M. K. Raja. Phishing: message appraisal and the exploration of fear and self-confidence. *Behaviour & Information Technology*, 39(11):1204–1224, November 2020.

[97] Ivana Hromatko, Mirjana Tonković, and Andrea Vranic. Trust in Science, Perceived Vulnerability to Disease, and Adherence to Pharmacological and Non-pharmacological COVID-19 Recommendations. *Frontiers in Psychology*, 12, 2021.

[98] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. Users' Perceptions of Chrome's Compromised Credential Notification. 2022.

[99] Daniel Jampen, Gürkan Gür, Thomas Sutter, and Bernhard Tellenbach. Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences*, 10(1):33, August 2020.

[100] Irving L Janis and Seymour Feshbach. EFFECTS OF FEAR-AROUSING COMMUNICATIONS. 1953.

[101] J Jansen and P van Schaik. Persuading End Users to Act Cautiously Online: Initial Findings of a Fear Appeals Study on Phishing. 2017.

[102] Jurjen Jansen and Paul Van Schaik. The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, 123:40–55, March 2019.

[103] Jongkil Jeong, Joanne Mihelcic, Gillian Oliver, and Carsten Rudolph. Towards an improved understanding of human factors in cybersecurity. In *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, pages 338–345. IEEE, 2019.

[104] Allen Johnston and Merrill Warkentin. Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34:549–566, September 2010.

[105] Rashmi Ashish Kadam. Informed consent process: A step further towards making it meaningful! *Perspectives in Clinical Research*, 8(3):107–112, 2017.

[106] Melissa G. Keith, Louis Tay, and Peter D. Harms. Systems Perspective of Amazon Mechanical Turk for Organizational Research: Review and Recommendations. *Frontiers in Psychology*, 8, 2017.

[107] Lepe Khanum. Phishing emails analysis and design automatic text generation tool for writing and sending phishing mail. 2020.

[108] Muhammad Syafiq Kheruddin, Muhammad Adam Emir Mohd Zuber, and Muhammad Mukhlis Mohamad Radzai. Phishing Attacks: Unraveling Tactics, Threats, and Defenses in the Cybersecurity Landscape. preprint, Preprints, January 2024.

[109] Cheonsoo Kim and Sung-Un Yang. Like, comment, and share on Facebook: How each behavior differs from the other. *Public Relations Review*, 43(2):441–449, June 2017.

[110] Carole L. Kimberlin and Almut G. Winterstein. Validity and reliability of measurement instruments used in research. *American Journal of Health-System Pharmacy*, 65(23):2276–2284, December 2008.

[111] Gerjo Kok, L Kay Bartholomew, Guy S Parcel, Nell H Gottlieb, and María E Fernández. Finding theory- and evidence-based alternatives to fear appeals: Intervention Mapping. *International Journal of Psychology*, 49(2):98–107, April 2014.

[112] Dariusz Krok, Ewa Telka, Małgorzata Szcześniak, and Adam Falewicz. Threat Appraisal, Resilience, and Health Behaviors in Recovered COVID-19 Patients: The Serial Mediation of Coping and Meaning-Making. *International Journal of Environmental Research and Public Health*, 20(4):3649, February 2023.

[113] Katharina Krombholz, Heidelinde Hobel, Markus Huber, and Edgar Weippl. Advanced social engineering attacks. *Journal of Information Security and Applications*, 22:113–122, June 2015.

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

[115] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Cranor, and Jason Hong. Teaching Johnny not to fall for phish. *ACM Trans. Internet Techn.*, 10, May 2010.

[116] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Lessons from a real world evaluation of anti-phishing training. In *2008 eCrime Researchers Summit*, pages 1–12, October 2008. ISSN: 2159-1245.

[117] Youngsun Kwak, Seyoung Lee, Amanda Damiano, and Arun Vishwanath. Why do users not report spear phishing emails? *Telematics and Informatics*, 48:101343, May 2020.

[118] Arista Lahiri, Sweety Suman Jha, Arup Chakraborty, Madhumita Dobe, and Abhijit Dey. Role of Threat and Coping Appraisal in Protection Motivation for Adoption of Preventive Behavior During COVID-19 Pandemic. *Frontiers in Public Health*, 9:678566, July 2021.

[119] Sean T. Lawson, Sara K. Yeo, Haoran Yu, and Ethan Greene. The cyber-doom effect: The impact of fear appeals in the US cyber security debate. In *2016 8th International Conference on Cyber Conflict (CyCon)*, pages 65–80, Tallinn, Estonia, May 2016. IEEE.

[120] Yi Yong Lee, Chin Lay Gan, and Tze Wei Liew. Thwarting Instant Messaging Phishing Attacks: The Role of Self-Efficacy and the Mediating Effect of Attitude towards Online Sharing of Personal Information. *International Journal of Environmental Research and Public Health*, 20(4):3514, February 2023.

[121] Adrian Leguina. A primer on partial least squares structural equation modeling (PLS-SEM). *International Journal of Research & Method in Education*, 38(2):220–221, April 2015.

[122] Pavel Y. Leonov, Alexander V. Vorobyev, Anastasia A. Ezhova, Oksana S. Kotelyanets, Aleksandra K. Zavalishina, and Nikolay V. Morozov. The Main Social Engineering Techniques Aimed at Hacking Information Systems. In *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, pages 0471–0473, Yekaterinburg, Russia, May 2021. IEEE.

[123] Tian Lin, Daniel E. Capecci, Donovan M. Ellis, Harold A. Rocha, Sandeep Dommaraju, Daniela S. Oliveira, and Natalie C. Ebner. Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. *ACM Transactions on Computer-Human Interaction*, 26(5):1–28, October 2019.

[124] Xiaoxue Liu, Jiexin Zhang, Peidong Zhu, Qingping Tan, and Wei Yin. Quantitative cyber-physical security analysis methodology for industrial control systems based on incomplete information Bayesian game. *Computers & Security*, 102:102138, March 2021.

[125] Xin Luo, Richard Brody, Alessandro Seazzu, and Stephen Burd. Social Engineering: The Neglected Human Factor for Information Security Management. *Information Resources Management Journal*, 24(3):1–8, July 2011.

[126] Rachid Ait Maalem Lahcen, Bruce Caulkins, Ram Mohapatra, and Manish Kumar. Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, 3(1):10, April 2020.

[127] James E Maddux and Ronald W Rogers. Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of Experimental Social Psychology*, 19:469–479, September 1983.

[128] Azad M. Madni. Integrating humans with software and systems: Technical challenges and a research agenda. *Systems Engineering*, 13(3):232–245, 2010. _eprint: https://incose.onlinelibrary.wiley.com/doi/pdf/10.1002/sys.20145.

[129] Vincent F. Mancuso, Adam J. Strang, Gregory J. Funke, and Victor S. Finomore. Human Factors of Cyber Attacks: A Framework for Human-Centered Research. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 58(1):437–441, September 2014.

[130] Davit Marikyan and Savvas Papagiannidis. Protection Motivation Theory. 2023.

[131] Jaclyn Martin. Phishing in Dark Waters: A Quasi-Experimental Approach with Evaluating Cyber-Security Training for End-Users. 2019.

[132] Winter Mason and Siddharth Suri. Conducting behavioral research on Amazon's Mechanical Turk. *Behavior Research Methods*, 44(1):1–23, March 2012.

[133] Winter Mason and Duncan J. Watts. Financial incentives and the "performance of crowds". In *Proceedings of the ACM SIGKDD Workshop on Human Computation*, pages 77–85, Paris France, June 2009. ACM.

[134] Julia May. Get the Jab or Else: Examining the role of Fear Appeals in the Herman Cain Award subreddit using Protection Motivation Theory. 2023.

[135] Alexandra M. Mellis and Warren K. Bickel. Mechanical Turk Data Collection in Addiction Research: Utility, Concerns and Best Practices. *Addiction (Abingdon, England)*, 115(10):1960–1968, October 2020.

[136] Donna M. Mertens. *Research and evaluation in education and psychology: Integrating diversity with quantitative, qualitative, and mixed methods.* Sage publications, 2019.

[137] Andras Molnar. *SMARTRIQS: A Simple Method Allowing Real-Time Respondent Interaction in Qualtrics Surveys*. December 2018.

[138] Victor M. Montori, editor. *Evidence-based endocrinology*. Contemporary endocrinology. Humana Press, Totowa, N.J, 2006.

[139] Andrea C. Morales, Eugenia C. Wu, and Gavan J. Fitzsimons. How Disgust Enhances the Effectiveness of Fear Appeals. *Journal of Marketing Research*, 49(3):383–393, 2012. Publisher: American Marketing Association.

[140] Karoline Mortensen and Taylor L. Hughes. Comparing Amazon's Mechanical Turk Platform to Conventional Data Collection Methods in the Health and Medical Research Literature. *Journal of General Internal Medicine*, 33(4):533–538, April 2018.

[141] Aaron Moss1, Cheskie Rosenzweig, Jonathan Robinson, Shalom Jaffe1, and Leib Litman1. Is it Ethical to Use Mechanical Turk for Behavioral Research? Relevant Data from a Representative Survey of MTurk Participants and Wages. 2023.

[142] Hans-Jürgen Möller. Effectiveness studies: advantages and disadvantages. *Dialogues in Clinical Neuroscience*, 13(2):199–207, June 2011.

[143] Bilal Naqvi, Kseniia Perova, Ali Farooq, Imran Makhdoom, Shola Oyedeji, and Jari Porras. Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, 132:103387, September 2023.

[144] Dale M. Needham, David J. Sinopoli, Victor D. Dinglas, Sean M. Berenholtz, Radha Korupolu, Sam R. Watson, Lisa Lubomski, Christine Goeschel, and Peter J. Pronovost. Improving data quality control in quality improvement projects. *International Journal for Quality in Health Care*, 21(2):145–150, April 2009.

[145] Borgert Nele, Friedauer Jennifer, Böse Imke, Sasse Angela, M, and Elson Malte. The Study of Cybersecurity Self-Efficacy: A Systematic Literature Review of Methodology. 2021.

[146] Christopher Nguyen. LEARNING NOT TO TAKE THE BAIT: AN EXAMINATION OF TRAINING METHODS AND OVERLEARNING ON PHISHING SUSCEPTIBILITY. 2018.

[147] Van Nguyen. Attribution of Spear Phishing Attacks: A Literature Survey. *DTIC Document, Tech. Rep.*, August 2013.

[148] Calvin Nobles. Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, 9(3):71–88, December 2018.

[149] National Institute of Standards and Technology. The Phish Scale: NIST-Developed Method Helps IT Staff See Why Users Click on Fraudulent Emails. *NIST*, September 2020. Last Modified: 2020-09-18T09:34-04:00.

[150] Hilary I. Okagbue, Pelumi E. Oguntunde, Emmanuela C. M. Obasi, and Elvir M. Akhmetshin. Trends and usage pattern of SPSS and Minitab Software in Scientific research. *Journal of Physics: Conference Series*, 1734(1):012017, January 2021.

[151] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 6412–6424, Denver Colorado USA, May 2017. ACM.

[152] R.W. Outhwaite. Positivism, Sociological. In *International Encyclopedia of the Social & Behavioral Sciences*, pages 625–629. Elsevier, 2015.

[153] Yoon Soo Park, Lars Konge, and Anthony R. Artino. The Positivism Paradigm of Research. *Academic Medicine*, 95(5):690–694, May 2020.

[154] Bimal Parmar. Protecting against spear-phishing. *Computer Fraud & Security*, 2012(1):8–11, January 2012.

[155] Kathryn Parsons. Human Factors and Information Security: Individual, Culture and Security Environment. 2010.

[156] Chaitali Parulekar. Minimize Phishing Attacks: Securing Spear attacks. 06(06), 2019.

[157] Nisha Patel. An Empirical Assessment of Users' Information Security Protection Behavior towards Social Engineering Breaches. 2021.

[158] Donald G Perrin, Elizabeth Perrin, Brent Muirhead, and Muhammad Betz. INTERNATIONAL JOURNAL OF INSTRUCTIONAL TECHNOLOGY AND DISTANCE LEARNING. January 2015.

[159] Atieh Saberi Pirouz, Vladimir Rabotka, and Mohammad Mannan. FriendlyMail: Confidential and Verified Emails among Friends. 2014.

[160] Ronald C. Plotnikoff and Nick Higginbotham. Protection motivation theory and the prediction of exercise and low-fat diet behaviours among Australian cardiac patients. *Psychology & Health*, 13(3):411–429, May 1998.

[161] Michael L Ray and William L Wilkie. Fear: The Potential of an Appeal Neglected by Marketing. *Journal of Marketing*, 1970.

[162] Bibia Renee Redd. Using the protection motivation theory to examine the effects of obesity fear arousal on the physical activity of young adult female college students. 2012.

[163] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, and Mattia Mossano. An investigation of phishing awareness and education over time: When and how to best remind users. August 2020.

[164] Report. Verizon's 2016 Data Breach Investigations Report finds cybercriminals are exploiting human nature, April 2016.

[165] Report. IBM, 2022.

[166] Hyeun-Suk Rhee, Cheongtag Kim, and Young U. Ryu. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(8):816–826, November 2009.

[167] C Ringle, S Wende, and A Will. SmartPLS, 2005.

[168] Stefan A. Robila and James W. Ragucci. Don't be a phish: steps in user education. *ACM SIGCSE Bulletin*, 38(3):237–241, September 2006.

[169] R Rogers, John Cacioppo, and Richard Petty. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. pages 153–177. January 1983.

[170] Ronald W. Rogers. A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1):93–114, September 1975. Num Pages: 22 Place: Provincetown, Mass., etc., United States Publisher: Journal Press, etc.

[171] Jian Raymond Rui, Keqing Yang, and Juan Chen. Information Sources, Risk Perception, and Efficacy Appraisal's Prediction of Engagement in Protective Behaviors Against COVID-19 in China: Repeated Cross-sectional Survey. *JMIR Human Factors*, 8(1):e23232, January 2021.

[172] Fatima Salahdine, Zakaria El Mrabet, and Naima Kaabouch. Phishing Attacks Detection A Machine Learning-Based Approach. In *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 0250–0255, New York, NY, USA, December 2021. IEEE.

[173] Kofi Sarpong Adu-Manu, Richard Kwasi Ahiable, Justice Kwame Appati, and Ebenezer Essel Mensah. Phishing Attacks in Social Engineering: A Review. *Journal of Cyber Security*, 4(4):239–267, 2022.

[174] Mariah Schrum, Muyleng Ghuy, Erin Hedlund-botti, Manisha Natarajan, Michael Johnson, and Matthew Gombolay. Concerning Trends in Likert Scale Usage in Human-robot Interaction: Towards Improving Best Practices. *ACM Transactions on Human-Robot Interaction*, 12(3):1–32, September 2023.

[175] Sebastian W. Schuetz, Paul Benjamin Lowry, Daniel A. Pienta, and Jason Bennett Thatcher. The Effectiveness of Abstract Versus Concrete Fear Appeals in Information Security. *Journal of Management Information Systems*, 37(3):723–757, July 2020.

[176] Sebastian Walter Schuetz, Paul Benjamin Lowry, and Jason Bennett Thatcher. DEFENDING AGAINST SPEAR PHISHING: MOTIVATING USERS THROUGH FEAR APPEAL MANIPULATIONS. 2016.

[177] Anjum N. Shaikh, Antesar M. Shabut, and M.A. Hossain. A literature review on phishing crime, prevention review and investigation of gaps. In *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*, pages 9–15, Chengdu, China, 2016. IEEE.

[178] Gholamreza Sharifirad, Parastoo Yarmohammadi, Mohammad Ali Sharifabad, and Zohreh Rahaei. Determination of preventive behaviors for pandemic influenza A/H1N1 based on protection motivation theory among female high school students in Isfahan, Iran. *Journal of Education and Health Promotion*, 3:7–7, January 2014. Num Pages: 7-7 Place: Mumbai, Mumbai Publisher: Medknow Publications & Media Pvt. Ltd.

[179] Kim Bartel Sheehan. Crowdsourcing research: Data collection with Amazon's Mechanical Turk. *Communication Monographs*, 85(1):140–156, January 2018.

[180] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 373–382, Atlanta Georgia USA, April 2010. ACM.

[181] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 88–99, Pittsburgh Pennsylvania USA, July 2007. ACM.

[182] Jingyuan (Jolie) Shi and Sandi W. Smith. The effects of fear appeal message repetition on perceived threat, perceived efficacy, and behavioral intention in the extended parallel process model. *Health Communication*, 31(3):275–286, March 2016.

[183] Murtaza Ahmed Siddiqi, Wooguil Pak, and Moquddam A. Siddiqi. A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences*, 12(12):6042, January 2022. Number: 12 Publisher: Multidisciplinary Digital Publishing Institute.

[184] Amrita Sil, Jayadev Betkerur, and Nilay Kanti Das. P-Value Demystified. *Indian Dermatology Online Journal*, 10(6):745–750, November 2019.

[185] Ramandeep Singh. Critique Of The Impact Of Positivism On Modern Schooling Curriculum Processes In The Context Of Value Education. 2022.

[186] Mikko Siponen and Anthony Vance. Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems*, 23, May 2014.

[187] Slashnext. The State of Phishing. 2022.

[188] R F Soames Job. Effective and ineffective use of fear in health promotion campaigns. *American Journal of Public Health*, 78(2):163–167, February 1988.

[189] Peter Markus Spieth, Anne Sophie Kubasch, Ana Isabel Penzlin, Ben Min-Woo Illigens, Kristian Barlinn, and Timo Siepmann. Randomized controlled trials – a matter of design. *Neuropsychiatric Disease and Treatment*, 12:1341–1349, 2016. Num Pages: 1341-1349 Place: Auckland, United Kingdom Publisher: Taylor & Francis Ltd. Section: Review.

[190] Frank Stajano and Paul Wilson. Understanding scam victims: seven principles for systems security. *Communications of the ACM*, 54(3):70–75, March 2011.

[191] Nathalie Stembert, Arne Padmos, Mortaza S. Bargh, Sunil Choenni, and Frans Jansen. A Study of Preventing Email (Spear) Phishing by Enabling Human Intelligence. In *2015 European Intelligence and Security Informatics Conference*, pages 113–120, September 2015.

[192] Simon Stockhardt, Benjamin Reinheimer, Melanie Volkamer, Peter Mayer, Alexandra Kunz, Philipp Rack, and Daniel Lehmann. Teaching Phishing-Security: Which Way is Best? In Jaap-Henk Stockhardt and Stefan Katzenbeisser, editors, *ICT Systems Security and Privacy Protection*, volume 471, pages 135–149. Springer International Publishing, Cham, 2016. Series Title: IFIP Advances in Information and Communication Technology.

[193] Clare Sullivan. The 2014 Sony Hack and the Role of International Law. 8, 2014.

[194] Jerry Chih-Yuan Sun, Shih-Jou Yu, Sunny S. J. Lin, and Shian-Shyong Tseng. The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior*, 59:249–257, June 2016.

[195] Richard A. Swanson and Ed Holton, editors. *Research in organizations: foundations and methods of inquiry*. Berrett-Koehler Publishers, San Francisco, CA, 1st ed edition, 2005.

[196] Melanie B. Tannenbaum, Justin Hepler, Rick S. Zimmerman, Lindsey Saul, Samantha Jacobs, Kristina Wilson, and Dolores Albarracín. Appealing to fear: A meta-analysis of fear appeal effectiveness and theories. *Psychological Bulletin*, 141(6):1178–1204, November 2015.

[197] Jason Thomas. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. *International Journal of Business and Management*, 13:1, April 2018.

[198] Kai Florian Tschakert and Sudsanguan Ngamsuriyaroj. Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, 5(6):e02010, June 2019.

[199] Steffen Ullrich, Benjamin Stritter, and Konrad Rieck. Reading Between the Lines: Content-Agnostic Detection of Spear-Phishing Emails. In Hugo Gascon, editor, *Research in Attacks, Intrusions, and Defenses*, volume 11050, pages 69–91. Springer International Publishing, Cham, 2018. Series Title: Lecture Notes in Computer Science.

[200] Wojciech Urban. Studying human behaviour to prevent successful spear-phishing attempts. 2022.

[201] Anthony Vance, Mikko Siponen, and Seppo Pahnila. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, 49(3-4):190–198, May 2012.

[202] Ike Vayansky and Sathish Kumar. Phishing – challenges and solutions. *Computer Fraud & Security*, 2018:15–20, January 2018.

[203] Jingguo Wang, Tejaswini Herath, Rui Chen, Arun Vishwanath, and H. Raghav Rao. Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. *IEEE Transactions on Professional Communication*, 55(4):345–362, December 2012. Conference Name: IEEE Transactions on Professional Communication.

[204] Rochelle E Watkins, Feonagh C Cooke, Robert J Donovan, C Raina MacIntyre, Ralf Itzwerth, and Aileen J Plant. Influenza pandemic preparedness: motivation for protection among small and medium businesses in Australia. *BMC Public Health*, 7(1):157, December 2007.

[205] Rachel Westcott, Kevin Ronan, Hilary Bambrick, and Melanie Taylor. Expanding protection motivation theory: investigating an application to animal owners and emergency responders in bushfire emergencies. *BMC Psychology*, 5(1):13, April 2017.

[206] Emma J Williams and Adam N Joinson. Developing a measure of information seeking about phishing. *Journal of Cybersecurity*, 6(1):tyaa001, January 2020.

[207] Kaylene Williams. Fear appeal theory. 2012.

[208] Natasha M. Wojcicki. Phishing Attacks: Preying on Human Psychology to Beat the System and Developing Cybersecurity Protections to Reduce the Risks. *World Libraries*, 23(1), August 2019. Number: 1.

[209] Wombat Security Wombat Security. Annual State of Phish Report from Wombat Security Shows Simulated Phishing and Training Programs Driving Safer End-User Behavior, 2017.

[210] Ken Kwong-Kay Wong. Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS. 2013.

[211] C. Wou, B. Silarova, S. Griffin, and J.A. Usher-Smith. The associations between the response efficacy and objective and subjective change in physical activity and diet in the Information and Risk Modification trial. *Public Health*, 165:26–33, December 2018.

[212] Guobin Wu, Xiaopeng Deng, and Bingsheng Liu. Using fear appeal theories to understand the effects of location information of patients on citizens during the COVID-19 pandemic. *Current Psychology*, June 2021.

[213] Huichuan Xia, Yang Wang, Yun Huang, and Anuj Shah. "Our Privacy Needs to be Protected at All Costs": Crowd Workers' Privacy Experiences on Amazon Mechanical Turk. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):1–22, December 2017.

[214] Aiping Xiong, Robert W. Proctor, Weining Yang, and Ninghui Li. Embedding Training Within Warnings Improves Skills of Identifying Phishing Webpages. *Human Factors*, 61(4):577–595, June 2019. Publisher: SAGE Publications Inc.

[215] Tianhao Xu, Kuldeep Singh, and Prashanth Rajivan. Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks. *Applied Ergonomics*, 108:103908, April 2023.

[216] Ahmad Shidki Mat Yusoff, Fan Siong Peng, Fahmi Zaidi Abd Razak, and Wan Azani Mustafa. Discriminant Validity Assessment of Religious Teacher Acceptance: The Use of HTMT Criterion. *Journal of Physics: Conference Series*, 1529(4):042045, April 2020.

[217] van Zadelhoff, Kristin Lovejoy, and David Jarvis. Fortifying for the future. 2014.

[218] Olga A. Zielinska, Rucha Tembe, Kyung Wha Hong, Xi Ge, Emerson Murphy-Hill, and Christopher B. Mayhorn. One Phish, Two Phish, How to Avoid the Internet Phish: Analysis of Training Strategies to Detect Phishing Emails. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 58(1):1466–1470, September 2014. Publisher: SAGE Publications Inc.

[219] Ágnes Zsóka, Zsuzsanna Marjainé Szerényi, Anna Széchy, and Tamás Kocsis. Greening due to environmental education? Environmental knowledge, attitudes, consumer behavior and everyday pro-environmental activities of Hungarian high school and university students. *Journal of Cleaner Production*, 48:126–138, June 2013.

[220] Pranas Žukauskas, Jolita Vveinhardt, Regina Andriukaitienė, Pranas Žukauskas, Jolita Vveinhardt, and Regina Andriukaitienė. Philosophy and Paradigm of Scientific Research. In *Management Culture and Corporate Social Responsibility*. IntechOpen, April 2018.

Appendix A

EXPERIMENTS SURVEY

This study designs an experiment that is managed via Qualtrics survey. It has four groups: education intervention, fear appeal intervention, educational-fear appeal intervention, and control group. The participants are assigned randomly to one of the four groups. All participants have the same questions, but each of them has different interventions. Figure 1 explains the questions flow for each group.

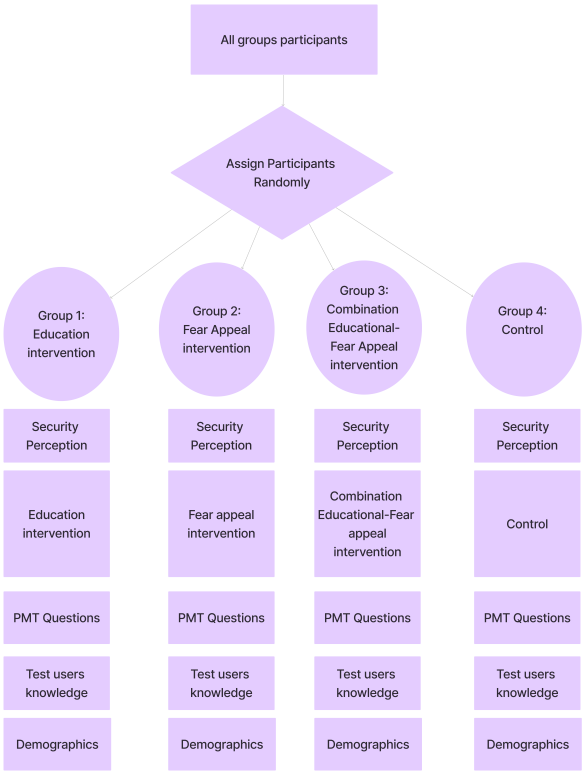


Figure A.1: Survey flow for all four groups

Survey Introduction

Effect of Education and Fear Appeal Scenario Against Spear Phishing Attacks Experiment. Survey on Education instrument, Fear Appeal scenarios against spear phishing attacks.

The following questionnaire is part of a research project to better understand the effect of education and fear appeal on users' behaviors against spear phishing attacks. Completing the whole survey will take about 10-20 minutes. This survey is completely voluntary. If you come to a question you do not want to answer, please feel free to skip to the next question. However, keep in mind some questions are required due to the use of logic. If you do not wish to answer those questions, then please discontinue your participation in the survey.

You may discontinue participation at any time and for any reason, including after the completion of the survey. In the event that you choose to stop participation, you may ask me to have your answers deleted by contacting me through email. Please take note of the date and time you worked on the survey for this purpose. All information shared in any publications or presentations will be anonymous in order to preserve your right to privacy.

Compensation will be received through the Amazon Mechanical Turk system and is limited to the amount noted therein–$2.00. No other compensation will be provided. This research does not involve risks beyond those encountered in daily life. If you have any questions or concerns, please contact the researcher at the email address below, or the UW Human Subjects Division.

Student Advisor: Marc Dupuis (marcjd@uw.edu) Project contact address: c/o Marc Dupuis, Computing and Software Systems, Box 358534, 18115 Campus Way NE, Bothell, WA 98011-8246. Investigator: Saja Alsulami (saja1998@uw.edu).

Please note: This survey will take some time. There are multiple quality control questions throughout the survey. If you fail a single quality control question then the survey will end and you will not be paid; this is done to preserve your Amazon Mechanical Turk rating. Your responses to that point will subsequently be discarded as they are unusable. If you do not think you have the time or ability to accurately complete a longer survey then please do

not proceed.

Additionally, if you use tools, AI, or anything else to automate your answers then you will be unable to complete future project with me.

CONSENT TO SURVEY PARTICIPATION

YOU MUST BE 18 YEARS OF AGE OR OLDER TO PARTICIPATE!

I certify that I am 18 years of age or older, that I can print out a copy of this consent form or otherwise save its contents by copying and pasting into a new document, that I have read the preceding, and that I understand its contents. By clicking on the next button, I am freely agreeing to participate in this study by filling out the survey.

NOTE: If you do not wish to participate in this survey then please close your browser window at this time

Security Perception

Please continue to answer each question honestly, on your own, and to the best of your ability, without assistance from any outside sources. Remember, all responses are completely anonymous.

Please rate the extent to which you agree with the following statement:

1. You have a clear understanding of "Spear Phishing attacks," and you are able to define it [89].

    - Strongly disagree
    - Somewhat disagree
    - Neither agree nor disagree
    - Somewhat agree
    - Strongly agree

2. Which of the following best defines the term "Spear Phishing attacks"? [89]

    - A type of unauthorized software that disrupts the regular functionality of a person's or organization's computer system, or corrupts or steals confidential data, or allows a cyber criminal to gain unauthorized access to a private computer system.
    - A practice of gathering helpful information about a targeted employee within an organization to deceive this employee to providing cyber criminals access to unauthorized, sensitive, and private data through a fake solicitation email, website link, text message, etc.
    - A specific type of software that prevents authorized users from accessing their files by penetrating a person or organization's computer systems, encrypting all files, and sending a copy of those files to the criminal's server.
    - An attack that prevents access for legitimate users when a targeted host or server is overloaded with traffic until the target cannot respond or crashes.

3. How do you assess your overall ability to defend against spear phishing attacks targeting specific individuals to steal credentials and commit fraud?[72]

    - Terrible
    - Poor
    - Average
    - Good
    - Excellent

4. Have you been the victim of at least one spear phishing attack in the past year in which user credentials were compromised and/or fraud was committed?[72]

    - No

- Maybe
- Yes

5. Have you ever checked these components in emails that you received?[200]

	Never	Sometimes	About half the time	Most of the time	Always
The Sender's email address	•	•	•	•	•
The Sender's name	•	•	•	•	•
The content of the email links	•	•	•	•	•
The content of the attachments	•	•	•	•	•
The content of the email pictures	•	•	•	•	•
The content of the email text	•	•	•	•	•

After these security perception questions, all groups will affected by different intervention types:

1. The first group was affected by an Education Intervention
2. The second group was affected by a Fear Appeal Intervention
3. The third group was affected by a combination of Educational-Fear Appeal Intervention
4. The fourth group was not affected by any type of the previous interventions.

Group 1: Education Intervention

In this video, you will learn about spear phishing attacks. Please watch the video below. `https://www.youtube.com/watch?v=zv19Azmumng`.

Common examples of spear phishing attacks:

1. Chief Executive Officer fraud scams Common spear phishing attack
2. Malicious attachments and ransomware attacks
3. Clone phishing attack, which is a type of spear phishing attack
4. Brand impersonation attack, which is a type of spear phishing attack

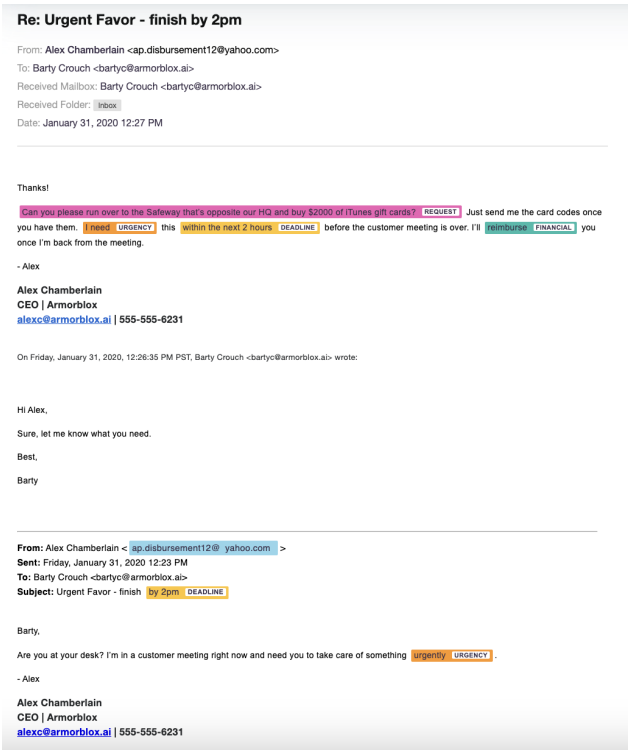


Figure A.2: CEO Fraud Scams

[50]

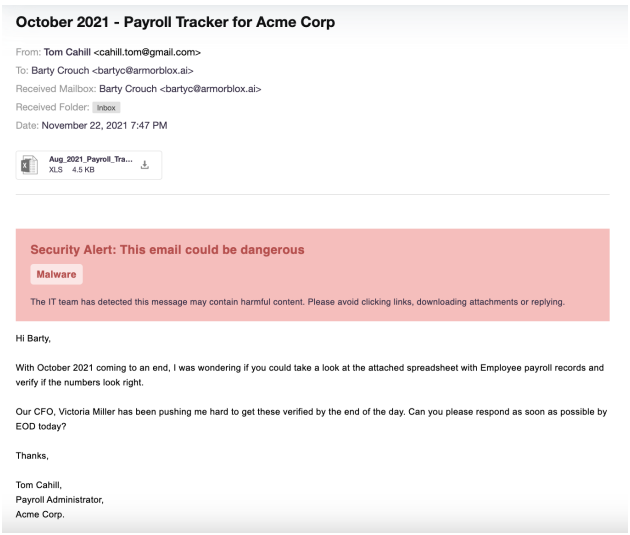


Figure A.3: Malicious Attachments

[50]

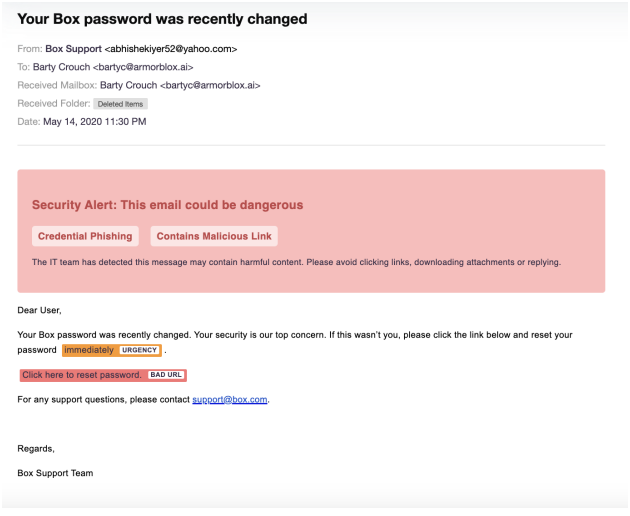


Figure A.4: Clone phishing attack

[50]

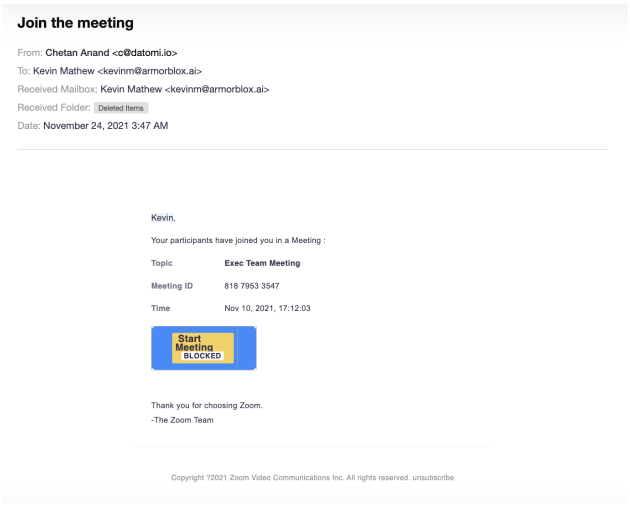


Figure A.5: Brand impersonation attack

[50]

Group 2: Fear Appeal Intervention

Spear phishing attacks:

A practice of gathering helpful information about a targeted employee within an organization for the purpose of deceiving this employee to provide cybercriminals access to sensitive and private data through a fake solicitation email[89].

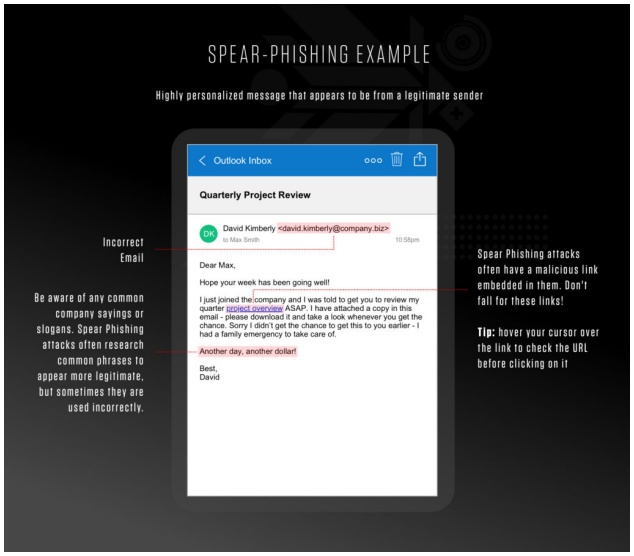


Figure A.6: Spear phishing Example

[1]

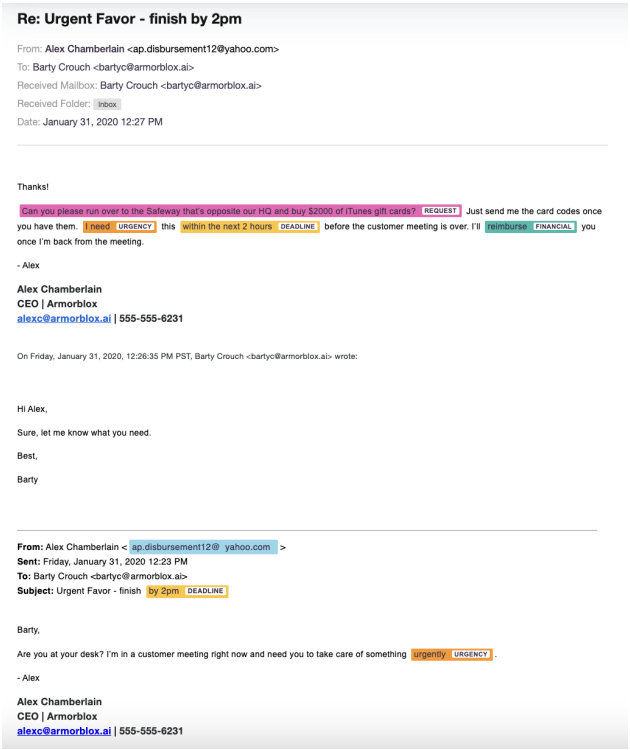
In this video, you will learn about spear phishing attacks. Please watch the video below: `https://www.youtube.com/watch?v=XJDyDN3HtOO`.

Group 3: Combination Educational-Fear Appeal Intervention

In this video, you will learn about spear phishing attacks. Please watch the video below. `https://www.youtube.com/watch?v=zv19Azmumng`.

Common examples of spear phishing attacks:

1. Chief Executive Officer fraud scams Common spear phishing attack
2. Malicious attachments and ransomware attacks
3. Clone phishing attack, which is a type of spear phishing attack
4. Brand impersonation attack, which is a type of spear phishing attack



Re: Urgent Favor - finish by 2pm

From: Alex Chamberlain <ap.disbursement12@yahoo.com>
To: Barty Crouch <bartyc@armorblox.ai>
Received Mailbox: Barty Crouch <bartyc@armorblox.ai>
Received Folder: Inbox
Date: January 31, 2020 12:27 PM

Thanks!

Can you please run over to the Safeway that's opposite our HQ and buy $2000 of iTunes gift cards? REQUEST Just send me the card codes once you have them. I need URGENCY this within the next 2 hours DEADLINE before the customer meeting is over. I'll reimburse FINANCIAL you once I'm back from the meeting.

- Alex

Alex Chamberlain
CEO | Armorblox
alexc@armorblox.ai | **555-555-6231**

On Friday, January 31, 2020, 12:26:35 PM PST, Barty Crouch <bartyc@armorblox.ai> wrote:

Hi Alex,

Sure, let me know what you need.

Best,

Barty

From: Alex Chamberlain < ap.disbursement12@ yahoo.com >
Sent: Friday, January 31, 2020 12:23 PM
To: Barty Crouch <bartyc@armorblox.ai>
Subject: Urgent Favor - finish by 2pm DEADLINE

Barty,

Are you at your desk? I'm in a customer meeting right now and need you to take care of something urgently URGENCY .

- Alex

Alex Chamberlain
CEO | Armorblox
alexc@armorblox.ai | **555-555-6231**

Figure A.7: CEO Fraud Scams

[50]

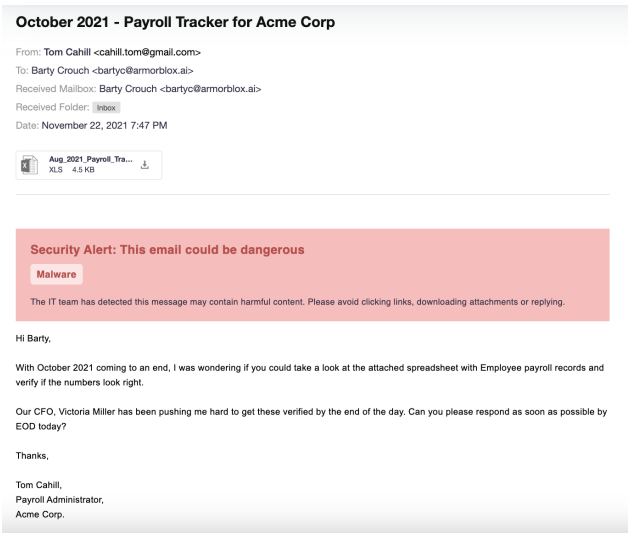


Figure A.8: Malicious Attachments

[50]

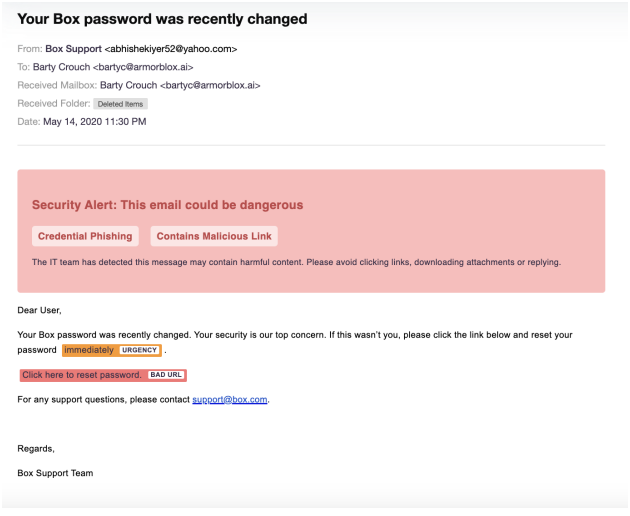


Figure A.9: Clone phishing attack

[50]

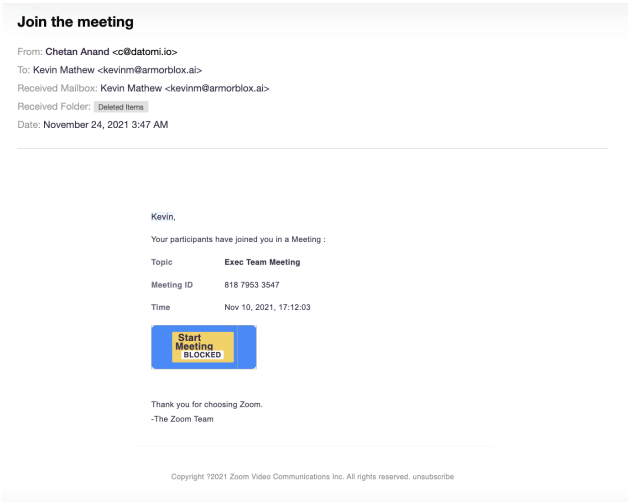


Figure A.10: Brand impersonation attack

[50]

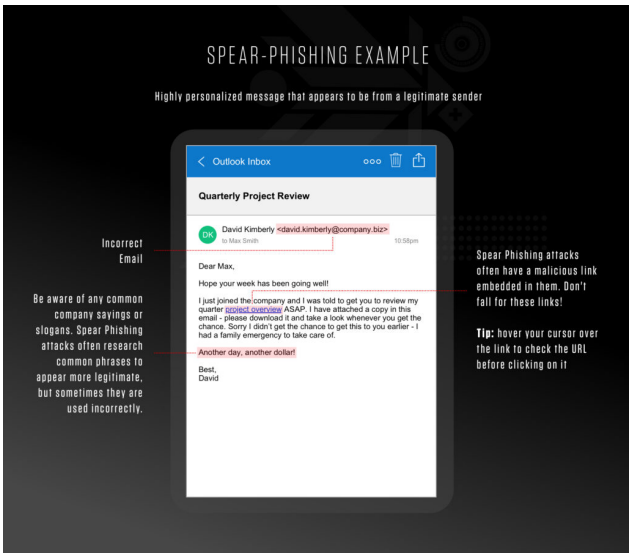


Figure A.11: Spear phishing Example

[1]

In this video, you will learn about spear phishing attacks. Please watch the video below: https://www.youtube.com/watch?v=XJDyDN3HtOO.

Group 4: Control Group

Please watch the video below:
https://www.youtube.com/watch?v=E1UViIQRqQU.

After being affected by different interventions, the participants have to answer PMT questions, Test their knowledge about spear phishing attacks, and answer Demographic questions.

PMT Question

Please rate the extent to which you agree with the following statements:

1. Threat severity

    - If I would fall victim to a spear phishing attack, the consequences would be severe.
    - If I would fall victim to a spear phishing attack, the consequences would be serious.
    - If I would fall victim to a spear phishing attack, the consequences would be significant. [1=Strongly disagree;7=Strongly agree][176]

2. Threat vulnerability

    - I am at risk of falling victim to a spear phishing attack.
    - There is a chance that I will fall victim to a spear phishing attack.
    - It is possible that I fall victim to a spear phishing attack.[1=Strongly disagree;7=Strongly agree][176]

3. Response efficacy

    - Looking for suspicious cues in emails works for protection against spear phishing attacks.
    - Verifying the legitimacy of an email is effective for protection against spear phishing attacks. carefully inspecting suspicious emails, my privacy is more likely to be protected. [1=Strongly disagree;7=Strongly agree][176]

4. Self-efficacy

    - Detecting spear phishing attacks is easy to do.
    - Detecting spear phishing attacks is convenient to do.

- I am able to detect spear phishing attacks without much effort. [1=Strongly disagree;7=Strongly agree][176]

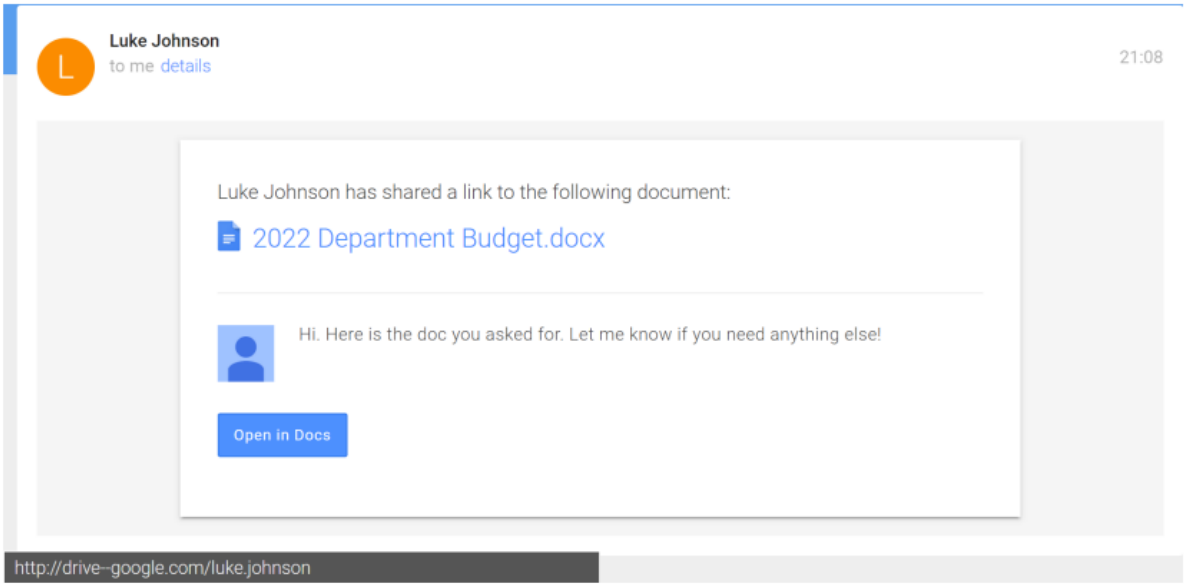
5. Response cost

- I would be discouraged from carefully inspecting every email because it would take too much time.
- Taking time to carefully verify every email would cause me too many problems.
- I would be discouraged from examining every email because I would feel silly to do so.[1=Strongly disagree;7=Strongly agree][176]

Test your knowledge about spear phishing attacks

This section will show eight examples of spear phishing and legitimate emails. This section is designed to test your knowledge to identify spear phishing and legitimate emails based on what you read and learned in the previous sections.

Please read the following questions carefully and respond based on this email.



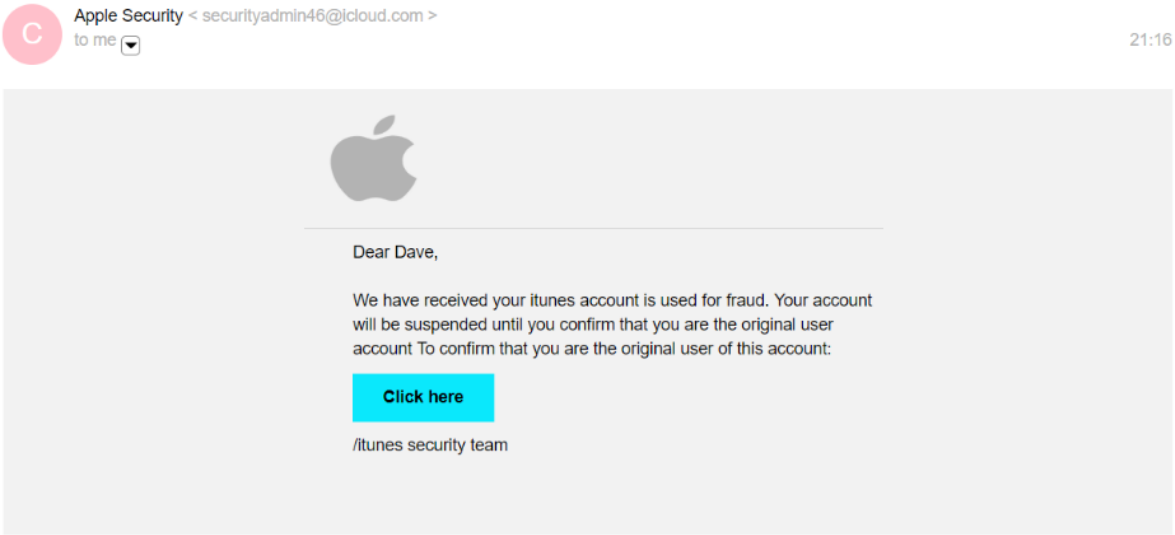
Email 1: An Example of Spear Phishing Email [200].

Question 1: Please indicate whether the email appears to be a spear phishing attack or is legitimate [27].

- Spear phishing email
- Legitimate email

If this email is spear phishing, then on a scale of 1-5, which factors lead you to believe this email to be spear phishing? [27]

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
Link in the email:	•	•	•	•	•
Text of email:	•	•	•	•	•
Attachment of the email:	•	•	•	•	•
Where the email came from:	•	•	•	•	•



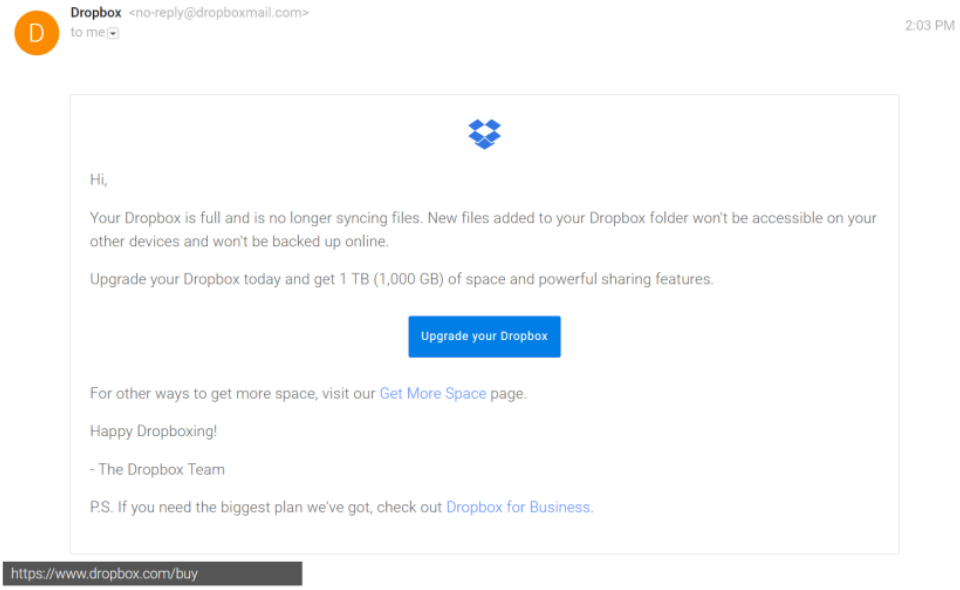
Email 2: An Example of Spear Phishing Email [74].

Question 2: Please indicate whether the email appears to be a spear phishing attack or is legitimate [27].

- Spear phishing email
- Legitimate email

If this email is spear phishing, then on a scale of 1-5, which factors lead you to believe this email to be spear phishing? [27]

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
Link in the email:	•	•	•	•	•
Text of email:	•	•	•	•	•
Attachment of the email:	•	•	•	•	•
Where the email came from:	•	•	•	•	•



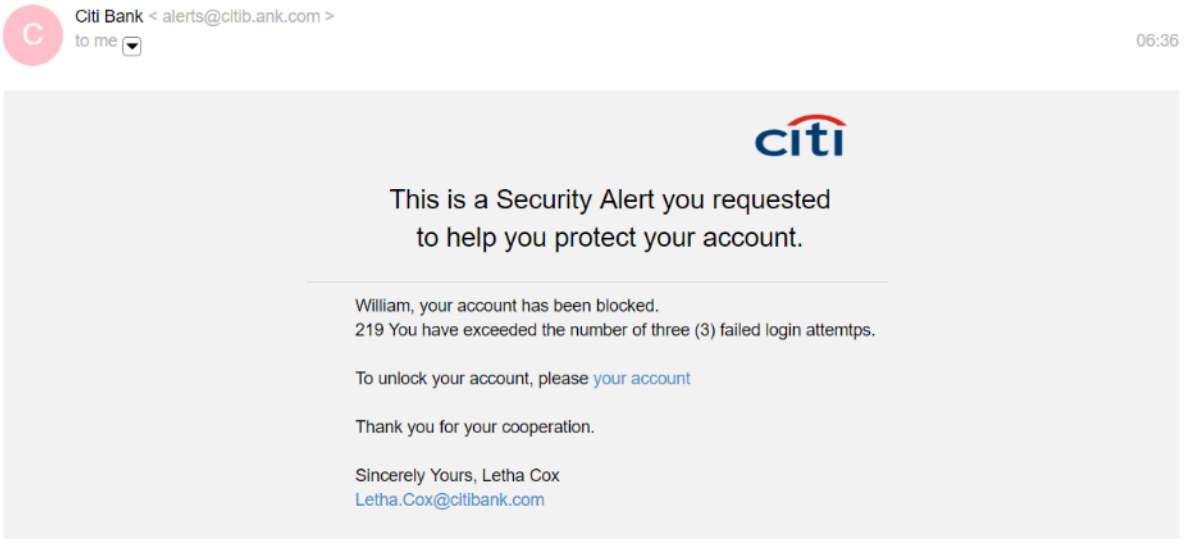
Email 3: An Example of Legitimate Email [200].

Question 3: Please indicate whether the email appears to be a spear phishing attack or is legitimate. [27]

- Spear phishing email
- Legitimate email

If this email is spear phishing, then on a scale of 1-5, which factors lead you to believe this email to be spear phishing? [27]

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
Link in the email:	•	•	•	•	•
Text of email:	•	•	•	•	•
Attachment of the email:	•	•	•	•	•
Where the email came from:	•	•	•	•	•



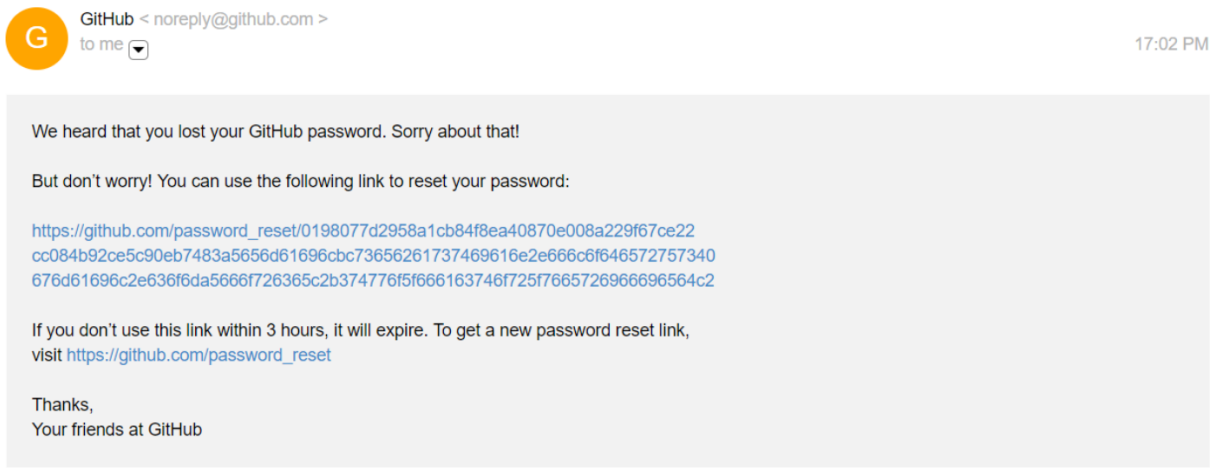
Email 4: An Example of Spear Phishing Email [74].

Question 4: Please indicate whether the email appears to be a spear phishing attack or is legitimate [27].

- Spear phishing email
- Legitimate email

If this email is spear phishing, then on a scale of 1-5, which factors lead you to believe this email to be spear phishing? [27].

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
Link in the email:	•	•	•	•	•
Text of email:	•	•	•	•	•
Attachment of the email:	•	•	•	•	•
Where the email came from:	•	•	•	•	•



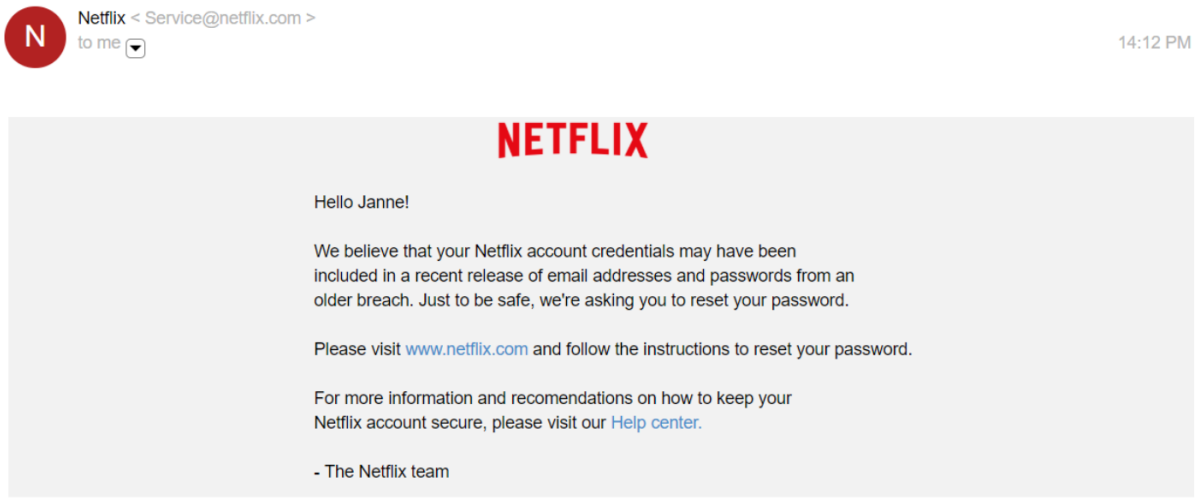
Email 5: An Example of Legitimate Email [74].

Question 5: Please indicate whether the email appears to be a spear phishing attack or is legitimate [27].

- Spear phishing email
- Legitimate email

If this email is spear phishing, then on a scale of 1-5, which factors lead you to believe this email to be spear phishing? [27]

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
Link in the email:	•	•	•	•	•
Text of email:	•	•	•	•	•
Attachment of the email:	•	•	•	•	•
Where the email came from:	•	•	•	•	•



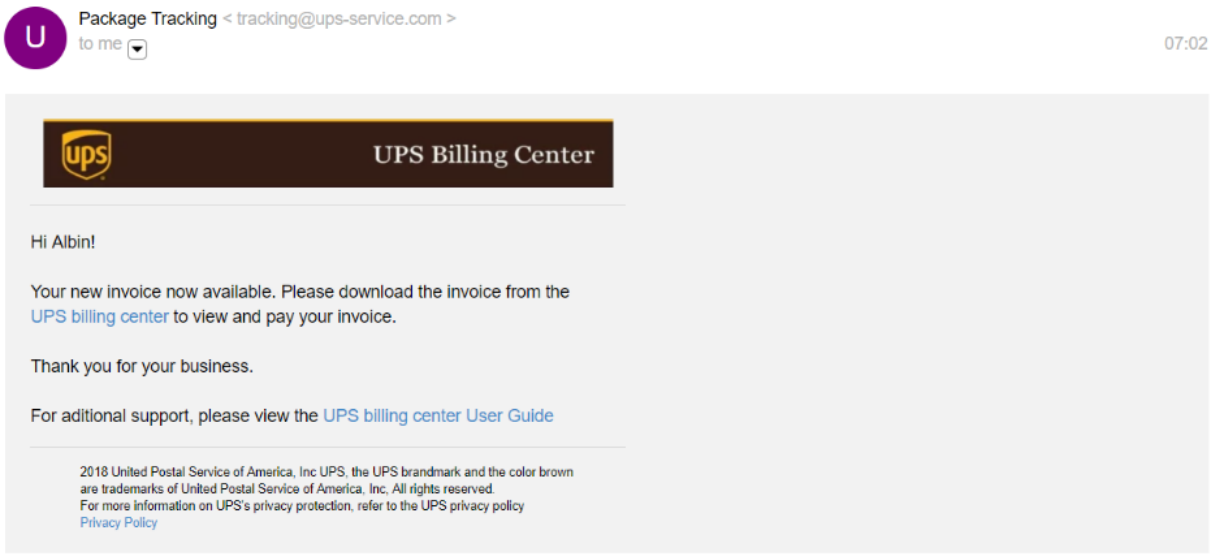
Email 6: An Example of Legitimate Email [74].

Question 6: Please indicate whether the email appears to be a spear phishing attack or is legitimate [27].

- Spear phishing email
- Legitimate email

If this email is spear phishing, then on a scale of 1-5, which factors lead you to believe this email to be spear phishing? [27]

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
Link in the email:	•	•	•	•	•
Text of email:	•	•	•	•	•
Attachment of the email:	•	•	•	•	•
Where the email came from:	•	•	•	•	•



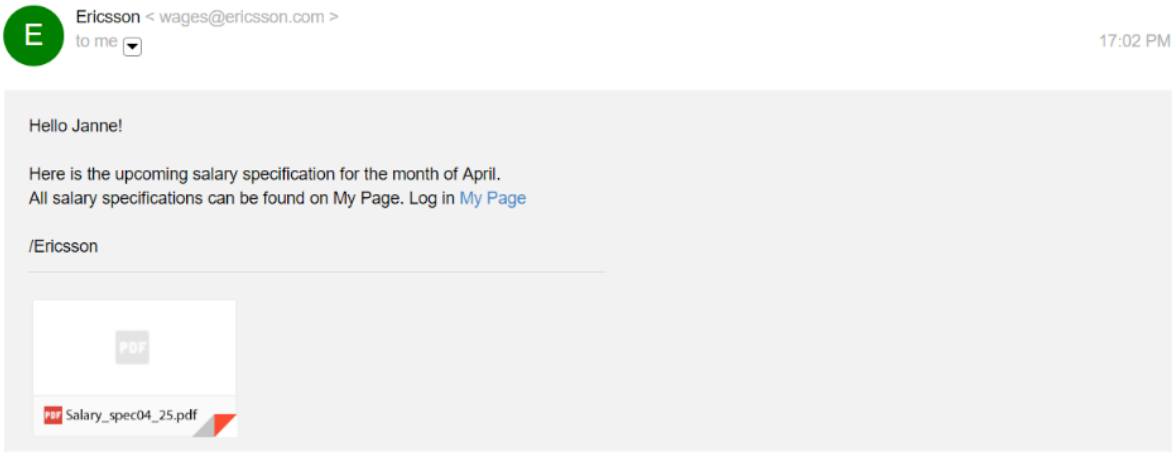
Email 7: An Example of Spear Phishing Email [74].

Question 7: Please indicate whether the email appears to be a spear phishing attack or is legitimate [27].

- Spear phishing email
- Legitimate email

If this email is spear phishing, then on a scale of 1-5, which factors lead you to believe this email to be spear phishing? [27]

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
Link in the email:	•	•	•	•	•
Text of email:	•	•	•	•	•
Attachment of the email:	•	•	•	•	•
Where the email came from:	•	•	•	•	•



Email 8: An Example of Legitimate Email [74].

Question 8: Please indicate whether the email appears to be a spear phishing attack or is legitimate [27].

- Spear phishing email
- Legitimate email

If this email is spear phishing, then on a scale of 1-5, which factors lead you to believe this email to be spear phishing? [27]

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
Link in the email:	•	•	•	•	•
Text of email:	•	•	•	•	•
Attachment of the email:	•	•	•	•	•
Where the email came from:	•	•	•	•	•

Demographics

1. What gender do you most closely identify with?
    - Female
    - Male
    - Non-Binary
    - Other
    - Prefer not to say

2. What is your current age?

    - Under 18
    - 18-19
    - 20-24
    - 25-29
    - 30-34
    - 35-39
    - 40-44
    - 45-49
    - 50-54
    - 55-59
    - 60-64
    - 65-69
    - 70-74
    - 75-79
    - 80-84
    - 85-89
    - 90 & above

3. What ethnicity do you primarily identify with?

    - Asian/Pacific Islander
    - Black/African-American
    - White/Caucasian

- Hispanic/Latinx
- Native American/Alaskan Native
- Other/Multi-Racial

4. What is the highest level of education you have obtained?

- Did not graduate high school (12th grade or less)
- Graduated high school or equivalent (GED)
- Some college, no degree
- Associate degree
- Bachelor's degree
- Master's degree
- Law degree, M.B.A., or other professional degree
- Doctorate degree

5. What is your current employment status?

- Employed full-time
- Employed part-time
- Not employed, looking for work
- Not employed, NOT looking for work
- Student, working at least part-time
- Student, NOT working