UNDERSTANDING SUSCEPTIBILITY TO SOCIAL ENGINEERING ATTACKS THROUGH ONLINE PRIVACY BEHAVIORS

by

Glaris Lancia Raja Arul

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Computer and Information Technology

West Lafayette, Indiana

December 2021

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Ida B. Ngambeki, Chair

Department of Computer and Information Technology

Dr. Kathryn C. Seigfried-Spellar

Department of Computer and Information Technology

Dr. Marcus Rogers

Department of Computer and Information Technology

Approved by:

Dr. John A. Springer

Dedicated to my Appa, the epitome of perseverance and sacrifice

ACKNOWLEDGMENTS

I would first like to thank my family and friends for their constant support and encouragement throughout my graduate study. To my parents, thank you both for your love, patience, and continued prayers. To my sister, my number one confidante, I am beyond grateful to you for all the conversations, reassurances, and caffeine indulgences. Thank you for helping me stay centered throughout the process of writing this thesis. Without all your support and belief in me, I wouldn't be where I am today. To my friends (you all know who you are), thank you all for constantly keeping me on my toes and challenging me to be the best person that I can be. I couldn't have asked for a better time at Purdue with all of you, near and far.

I would like to extend my heartfelt gratitude to my advisor, Dr Ida Ngambeki. I honestly do not know where to begin with how grateful I am for your support and guidance throughout the development and completion of this thesis. This acknowledgement of thanks does not fully encompass how deeply appreciative I am for the opportunity to know, learn from, and work with you. I've learnt a great deal from you about what it means to be a researcher and an educator, and I hope to do you proud in all my future endeavors.

I would also like to thank my committee members, Dr Kathryn Seigfried-Spellar and Dr Marcus Rogers, for all their feedback and assistance on this thesis. Your insights greatly helped in the refinement of this thesis, and I want to thank you both for lending your expertise and helping me improve the quality of my work.

Finally, I would also like to thank one of my first college educators, Professor Emerita Guity Ravai. I will never forget how you saw potential in me as a freshman, and constantly encouraged my different academic and extracurricular pursuits during my undergraduate years. I will always cherish your affirmations and support.

TABLE OF CONTENTS

TABLE OF CONTENTS 5
LIST OF TABLES 7
LIST OF FIGURES 8
LIST OF ABBREVIATIONS 9
GLOSSARY 10
ABSTRACT 11
CHAPTER 1. INTRODUCTION 12
1.1 Background 12
1.2 Statement of Problem 14
1.3 Research Question 14
1.4 Hypotheses 14
1.5 Significance of Problem 15
1.6 Scope 15
1.7 Assumptions 16
1.8 Limitations 16
1.9 Delimitations 16
CHAPTER 2. LITERATURE REVIEW 17
2.1 Social Engineering in Cybersecurity 17
2.2 Factors Influencing Susceptibility to Social Engineering 20
2.3 Countermeasures against Social Engineering 23
2.4 Defining Privacy in the Online Space 24
2.5 Factors Influencing Online Privacy 26
2.6 The Relationship between Social Engineering and Privacy 30
2.7 Theoretical Framework 31
2.7.1 Protection Motivation Theory 32
2.7.2 The Psychological Need for Privacy 34
2.8 Research Model 35
CHAPTER 3. METHODOLOGY 39
3.1 Research Design 39

3.2 Population and Sample 40
3.3 Measures of Variables 40
3.3.1 Measures of Demographic Variables 40
3.3.2 Measure of Social Engineering Victimization 41
3.3.3 Measure of Need for Privacy 41
3.3.4 Measure of Privacy Self-Efficacy 42
3.3.5 Measure of Privacy Response Efficacy 42
3.3.6 Measure of Privacy Protective Behaviors 43
3.3.7 Measure of Susceptibility to SE Attacks 43
3.4 Validity and Reliability of Adapted Measures 45
3.5 Validity and Reliability of SE Susceptibility Scale 47
CHAPTER 4. DATA ANALYSIS AND RESULTS 51
4.1 Data Screening 51
4.2 Descriptive Statistics 51
4.3 Analytical Strategies 54
4.4 Analysis Results 54
4.5 Summary of Results 63
CHAPTER 5. DISCUSSION 65
5.1 Discussion of Demographics 65
5.2 Discussion of Hypothesis 1 66
5.3 Discussion of Hypothesis 2 67
5.4 Discussion of Hypothesis 3 68
5.5 Discussion of Hypothesis 4 69
5.6 Discussion of Hypothesis 5 70
5.7 Discussion of Mediation Model 71
CHAPTER 6. CONCLUSION AND FUTURE WORK 72
6.1 Limitations 72
6.2 Conclusions and Future Work 73
REFERENCES 76
APPENDIX: RESEARCH SURVEY 89

LIST OF TABLES

Table 3.1 Factor loadings and communalities based on principal components analysis for 21 items on Susceptibility to Social Engineering Scale (n = 272) 48

Table 3.2 Factor loadings and communalities based on principal components analysis for 7 items on Susceptibility to Smishing Subscale (n = 272) 49

Table 3.3 Factor loadings and communalities based on principal components analysis for 7 items on Susceptibility to Phishing Subscale (n = 272) 49

Table 3.4 Factor loadings and communalities based on principal components analysis for 7 items on Susceptibility to Pharming Subscale (n = 272) 50

Table 4.1 Demographics for self-reported SE non-victims versus victims 52

Table 4.2 Summary of frequency analyses on study variables 53

Table 4.3 Zero-order correlations between victimization and average susceptibilities scores 55

Table 4.4 Results of independent samples t-test 55

Table 4.5 Zero-order correlations between demographics, privacy protective behaviors, and susceptibility to SE attacks 56

Table 4.6 Zero-order correlations between study variables 57

Table 4.7 Summary of results of one-way MANOVA 58

Table 4.8 Multiple regression predicting engagement in privacy protective behaviors 59

Table 4.9 Summary of mediation analysis 63

LIST OF FIGURES

Figure 2.1 Research Model 35
Figure 3.1 Example of a Social Engineering Scenario 44
Figure 3.2 Example of a Legitimate Scenario 45
Figure 4.1 Model of Mediation Analysis 62

LIST OF ABBREVIATIONS

ANOVA	Analysis of Variance
IC3	Internet Crime Complaint Center
ICT	Information and Communication Technologies
MANOVA	Multivariate Analysis of Variance
NFP	Need for Privacy
PMT	Protection Motivation Theory
SE	Social Engineering

GLOSSARY

Need for Privacy: The need to selectively control the access of others to the individual self, with the aim of achieving a desired level of physical or psychological privacy (Trepte & Masur, 2020, p. 3132).

Online Privacy: The ability of individuals to decide how their information is communicated to others across online environments. This definition is adapted from Westin (2003) and mirrors the definition of information privacy provided by Bergmann (2008). More discussions on the development of the concept of online privacy is available in the literature review, but for the scope of this research study, online privacy and information privacy are considered synonymous.

Privacy Response Efficacy: In the scope of this thesis, "privacy response efficacy" is defined as the extent to which individuals perceive contemporary privacy protective measures being capable of reducing threats to online privacy.

Privacy Self Efficacy: An individual's perceived capability about engaging in the behaviors that are necessary to maintain their online privacy.

Social Engineering: "Social Engineering" in the scope of this thesis is broadly defined as the art of manipulating individuals into divulging personal or sensitive information through means of deceptive psychological and persuasive techniques (Krombholz et al., 2015).

ABSTRACT

Human-based social engineering attacks continue to grow in popularity, with increasing numbers of cases reported yearly. This can be accredited to the ease with which common social engineering attacks can be launched, and the abundance of information available online that attackers can use against their targets. Current mitigative strategies and awareness trainings against social engineering attacks incorporate an understanding of the major factors that influence individual susceptibility to social engineering attacks. These strategies emphasize an engagement in secure behaviors and practices, especially with respect to identifying the key indicators in any form of communication or situation that can classify it as a social engineering attack. There is also an emphasis on restricting the amount of information that individuals should share about themselves in workplace settings. However, these approaches do not comprehensively consider the different intrinsic motivations that individuals develop to engage in the protective behaviors necessary to assure their safety against social engineering attacks, regardless of environment. Individual attitudes and behaviors about online privacy could hold the key to defending oneself by way of restricting unwarranted access to associated information online. Psychological traits and attitudes developed in response to the perception of social engineering as a threat could act as motivators for engaging in privacy protective behaviors, which in turn could affect the extent to which an individual can protect themselves from social engineering attacks. This thesis investigates the role of privacy protective behaviors in impacting an individual's susceptibility to social engineering attacks and the impacts of specific privacy factors as motivating antecedents to engagement in privacy protective behaviors.

CHAPTER 1. INTRODUCTION

1.1 Background

Social engineering attacks remain prolific in cyberspace, despite growing awareness of the different types of attacks that can be executed against individuals and organizations alike. Social engineering attacks are effective because they take advantage of an individual's inherent behaviors and mannerisms, and leverage psychological principles and tactics, to fraudulently influence them into divulging personal, confidential information (Department of Homeland Security, 2020). The effectiveness of these attacks could certainly be attributed to the increased reliance on technology in the past year alone, owing to the novel coronavirus pandemic (Venkatesha et al., 2021). However, this is merely indicative of the increased magnitude of social engineering attacks with the increased adoption of technology across work, home and social environments.

According to the FBI's Internet Crime Complaint Center, the number of complaints reported about cyberattacks increased by 69% from the start of the novel coronavirus (COVID-19) pandemic, compared to complaints reported during 2019. In the same report, losses from these crimes were estimated to exceed $4.2 billion, and the most common type of crime that was reported was phishing scams (Internet Crime Complaint Center [IC3], 2021). Surveys conducted by companies and interest groups have indicated that social engineering is continually incorporated in technical and non-technical attacks (Fox, 2021). According to research conducted amongst cybersecurity professionals, 71% of respondents indicated that employees at their organizations had fallen victim to social engineering attacks over the past year (Electric, 2021). Some of the most common social engineering attacks like phishing, vishing and ransomware utilize knowledge about common behaviors to get individuals to execute malicious programs or provide personal information about themselves. As such, individuals largely tend to be the targets of these attacks, with the IC3 reporting close to a quarter of a million complaints about social engineering attacks filed in the last year alone. The consequences of SE attacks continue to be detrimental. The financial damages from cybercrimes across the world was estimated to cost $6 trillion annually from 2021 onwards. In the past year alone, damages from cybercrimes, including social engineering attacks, was reported to be over $1 trillion (McAfee, 2020). These include, but are not

limited to, losses from information breaches, reduced or lost efficiency, and damages to the reputation of the companies involved.

In response, there have been more calls for changes in how organizations and individuals alike prevent and mitigate the consequences of social engineering attacks. These strategies constitute actionable items, but still fall short because of the old adage in information security of humans being the weakest link in the security chain (Luo et al., 2011). This is what makes social engineering an attractive precursor or component in various kinds of cyber-attacks. The psychological and persuasive tactics employed in social engineering are geared towards influencing people to act in a predictable or specific manner that is harmful to their privacy and security (Krombholz et al., 2015). These attacks are further augmented by the wealth of information publicly available online about individuals. Attackers can use this publicly available information either to execute social engineering attacks, or to gain further personal information from secondary sources using what they know about their target. While this isn't to say that companies are complacent about the security habits of their employees, there is limited focus on the capabilities of individuals of performing preventative behaviors when considering their susceptibility to social engineering attacks. Academic research in this area is largely concerned with understanding motivations of information security behaviors to prevent vulnerability to social engineering attacks (Aldawood & Skinner, 2019; Tayouri, 2015).

The aim of this thesis was to understand individual's susceptibility to popular social engineering attacks through their privacy attitudes and beliefs surrounding their information online, and through the privacy protective behaviors that they might engage in to ensure control over the disclosure of their information. Engagement in these privacy protective behaviors could serve as a means of defense from social engineering attacks. While employees are asked to be mindful of their behaviors and partake in security trainings, there still exists a disparity between their training and actual behavior, as evidenced not only by the increase in cyberattacks but the increase in complaints through the years. People in general seem to care about their presence online and how much information they choose to divulge online, but seem to care less or do little to assure their online privacy, as opposed to their online security (Debatin et al., 2009; Nyoni & Velempini, 2018). This thesis first considered the role of specific factors guiding engagement in privacy protective behaviors, most notably the psychological Need for Privacy (NFP), the elements of privacy self-efficacy and privacy response efficacy respectively, adapted from Protection

Motivation Theory (PMT), past experiences with social engineering attacks, and any applicable demographic factors. The thesis then considered the role of the privacy protective behaviors specifically, and how engagement in these behaviors could influence the extent to which individuals are susceptible to commonly experienced and reported social engineering attacks.

1.2 Statement of Problem

Individuals continue to fall victim to social engineering attacks despite awareness campaigns and security audits. The expectation is that providers of online services like social media would assure the online privacy of individuals, but in reality, the responsibility does not fall on these entities alone. Individual's privacy beliefs and attitudes, and subsequent engagement in privacy protective behaviors, might hold the key to understanding the extent to which someone is susceptible to social engineering attacks.

1.3 Research Question

The research study explored the following research question:

1. Does engagement in privacy protective behaviors mediate the relationship between specific privacy antecedents and susceptibility to social engineering attacks?

1.4 Hypotheses

To answer the research question, this thesis tested the following hypotheses:

Individuals who engage in privacy protective behaviors are less likely to be susceptible to social engineering attacks

Individuals who score high on privacy self-efficacy are more likely to engage in privacy protective behaviors

Individuals who score high on privacy response efficacy are more likely to engage in privacy protective behaviors

Individuals who have been victims of social engineering attacks are more likely to engage in privacy protective behaviors

Individuals who score high on the need for privacy are more likely to engage in privacy protective behaviors

1.5 Significance of Problem

The major contribution of this study would be to understand the perceived impacts of the most common social engineering attacks on individuals through the lens of their privacy behaviors. Privacy by itself is highly contextual in nature, regardless of how it is perceived in online and offline environments. It stands to reason that a person's perception of their online privacy will change depending on the type of online environment that they have a presence in, inherent traits and dispositions, and external situational factors. The nature of online privacy is complex but can be understood in a comprehensive manner through specific situations or attacks that people are increasingly likely to encounter. With social engineering attacks on the rise, specifically attacks that target underlying psychological mannerisms of people and use public information against their targets, it is important to understand if the underlying attitudes that people have about their privacy, in conjunction with other factors, can actually determine whether they are capable in their abilities to identify social engineering attacks when presented with them and whether they actually engage in the protective behaviors that can shield them or alert them to social engineering attacks.

1.6 Scope

This thesis investigated susceptibility to social engineering attacks through privacy protective behaviors that individuals engage in, and select privacy factors that were hypothesized to influence engagement in privacy protective behaviors. This thesis considered the roles of privacy self-efficacy and privacy response efficacy, adapted from the coping appraisals discussed in Protection Motivation Theory, and the concept of the psychological need for privacy. PMT has been largely used to identify areas of improvement in the formation of security behaviors and the development of security awareness programs (Bada et al. 2019) but has seen little application towards understanding individual defenses against social engineering attacks. Using the PMT framework, this research will specifically consider an individual's self-efficacy pertaining to privacy, and their perceptions of the efficacy of existing countermeasures against threats to privacy, and relate it to the development of protective behaviors against social engineering and reported social engineering victimization. The effects of common demographic variables like age and gender will also be studied in conjunction with the measures to understand the effect of group

memberships across demographics on reported privacy protective behaviors and susceptibility to social engineering attacks.

1.7 Assumptions

The assumptions of this research are as follows:

- Individuals will accurately report their engagement in privacy protective behaviors
- Individuals will disclose whether they have been a victim of a social engineering attack
- Individuals will have experienced at least one type of social engineering attack (for example – receiving a phishing email)
- The threat appraisal of social engineering attacks is implied across the population based on attack reports and estimated losses

1.8 Limitations

The limitations of this research are as follows:

- The results of this research may not be generalizable globally, particularly in areas with low adoption of technology and decreased interaction with technology
- The results may not be reflective of the impacts of need for privacy and self-efficacy measures on all types of non-technical social engineering attacks
- This study used a convenience sample from MTurk, which is not truly representative of the internet user population

1.9 Delimitations

The delimitations of this research were as follows:

- Respondents were only solicited from the United States of America
- Only adults (from age 18 and up) were sampled for the research
- Susceptibility to social engineering was measured for the three most common types of social engineering attacks reported to IC3 during 2020.
- Survey respondents were asked about their engagement in privacy protective behaviors alone, as opposed to both privacy and security protective behaviors

CHAPTER 2. LITERATURE REVIEW

To address the main concepts of social engineering and online privacy as presented in the research question, the literature review provides an overview of social engineering and privacy as studied in the online space. The components of social engineering that are discussed in the review are the development of social engineering as a concept within cybersecurity, the different factors that influence individuals' susceptibility to social engineering attacks, and countermeasures against human-based social engineering attacks. This is followed by a discussion on what constitutes online privacy, the factors that influence individuals' online privacy concerns and behaviors, and the relationship between social engineering and online privacy. Following this, literature on the theoretical motivations for this research study is discussed. Based on the literature review, the research model and hypotheses are presented.

2.1 Social Engineering in Cybersecurity

The concept of social engineering was first used to refer to campaigns or actions that were undertaken to understand and change the behaviors of people in society for a specific cause. The premise behind the concept was motivated by the thought that for industries and societies to flourish, there was a vested need to understand the workings of people and improve upon their fallacies to address societal ills and solve issues (Hatfield, 2018). This basic premise of social engineering remains the same across all areas of applications, in terms of engineering the human element in a process to achieve a specific goal. In the field of information security, social engineering (SE) can be broadly defined as the art of manipulating individuals into divulging personal, sensitive information through means of deceptive psychological and persuasive techniques (Krombholz et al., 2015). Social engineering attacks are carried out deliberately and often with malicious intent. The goal of a social engineering attack is to elicit information from the target, whether that be confidential data or access to restricted systems (Breda et al., 2017). The tactics leveraged in such attacks can be executed independently or in conjunction with other technical or non-technical attacks. The main targets of social engineering attacks are people, as opposed to only technological infrastructures and systems. Technical social engineering attacks do target the systems but are usually preceded by an action on the part of the individual who has

access to or is a part of the system. These attacks also rely on the ubiquitous nature of information to be executable and successful.

Taxonomies of SE attacks vary depending on the established parameters of the attack, the specific type of attack, and attack vectors. The largely agreed upon classification of social engineering attacks is into two categories; human-based attacks and technology-based attacks (Peltier, 2006; Krombholz et al., 2015; Koyun & Al Janabi, 2017). Human-based social engineering attacks involve direct interactions between attackers and victims. The attacker directly utilizes persuasive techniques to influence their victims to act in a certain manner. There is face-to-face contact between the attacker and the victim. Technology-based social engineering attacks involve the use of technology to achieve the same results as a human-based social engineering attack, but there is usually no direct contact between the attacker and the victim. In light of this, both classes of attacks tend to use similar principles to make their targets respond according to the wishes of the attacker, specifically ones rooted in the principles of persuasion and psychological manipulation. Another taxonomy was suggested by Ivaturi and Janczewski (2011) to classify SE attacks based on the level of socialization of the attacker with the victim. This classification largely focused on person-person types of social engineering, with the distinction lying in the media through which the attacks are executed.

The most common types of social engineering attacks that have been reported in current times include phishing attacks, watering hole attacks, whaling attacks, pretexting, and baiting and quid pro quo attacks (Paganini, 2020). Of these, phishing, vishing, smishing, and pharming attacks were the most reported types of internet crime in 2020, with close to a quarter of a million attacks reported to IC3 by individuals and businesses (Internet Crime Complaint Center, 2021). In phishing attacks, attackers impersonate a legitimate or trusted entity in order to gain credentials from users. This occurs via email communications, and targets are often asked to either reply with the solicited information or click on a link that then requests the information (Ma, 2013). Vishing and smishing can be considered variants of phishing attacks, as the objectives of these attacks are the same but the medium through which the attack is executed is different. In vishing attacks, attackers call individuals and use false pretexts and impersonation to elicit sensitive information. Smishing occurs via text messages, with attackers asking individuals to click on fraudulent links to gain information. Pharming is another type of phishing attack but the difference is that the attack does not target individuals specifically. Rather, the attackers spoof genuine, popular websites in

order to “lure” individuals to the fraudulent website and harvest information from targets that unwittingly provide their information (Johansen, 2019). A watering hole attack is when the attacker compromises a legitimate website that is used frequently by their target, without the knowledge of the individual (NIST, 2020). Whaling attacks follow the same premises as phishing attacks, but the difference lies in who the attackers target as a part of their campaign. In whaling attacks, attackers target high-profile employees in companies like upper management and senior executives. This is different from phishing attacks, where the campaigns are directed at all kinds of people, regardless of whether they belong to an organization. Pretexting can be seen as a precursor to technical-based social engineering attacks, and is defined as the process of obtaining information using a false story, or a “pretext”. Pretexting requires a lot of intelligence gathering about the individual or organization prior to its execution (Ivaturi & Janczewski, 2011). Baiting is a form of social engineering where the attacker exploits their target’s innate curiosity to then deceive them. Unlike some of the other attacks discussed, baiting can also be implemented physically. An example of this is leaving USBs with malicious programs across office spaces labeled “confidential” and waiting for employees to pick up the USBs and insert them into their work machines. As the name suggests, in quid pro quo attacks, the attackers promise some type of good or service, particularly something that is of benefit to their target, in exchange for the execution of the specific action that the attacker wants (Paganini, 2020).

Some of the attacks discussed above allude to the importance of collecting information about targets before executing the attack itself. This is because the success of social engineering attacks lies in how influential the attackers can be over their targets. To achieve this, attackers need to know their targets. If their targets get suspicious about the nature of interactions, then the attack would be less likely to succeed. Attackers can peruse publicly available information from places like company websites, and social and professional networking platforms. The continued rise in data breaches (Bissell et al., 2019), and lack of awareness amongst most of the American public about the potential compromise of their accounts (Sobers, 2020), leaves individuals more vulnerable and susceptible to social engineering attacks, and benefits attackers by making information more accessible for further development of non-technical and technical attacks.

2.2 Factors Influencing Susceptibility to Social Engineering

Apart from technological means and intelligence gained from public sources, attackers can also leverage psychological tactics to influence their targets into divulging information and/or executing a certain action. From the behavioral psychology standpoint, attackers take advantage of known human qualities like the desire to help others, tendencies to trust, aversion to trouble, prioritization of convenience, and general obedience to authority (Peltier, 2006). Elements of social psychology can also be seen through the employment of persuasive strategies and the exploitation of commonly held attitudes and behaviors. This is commonly seen in applications of persuasion concepts like Cialdini's principles of persuasion to understand why individuals are prone to persuasion and how attackers take advantage of these mannerisms to persuade individuals for their malicious intent (Schaab et al., 2017; Uebelacker & Quiel, 2014). This in turn can help with understanding which individuals, along with other internal and external factors associated with them, are most susceptible to social engineering attacks. To operationalize susceptibility to social engineering attacks, susceptibility in the context of this research refers to whether a person has the potential to fall victim to an SE attack. Measures of susceptibility in information security research have been absolute or implied. Counts of individuals clicking on phishing links is an example of a measure of absolute susceptibility. Individuals misclassifying a presented email as a non-phishing email constitutes an example of a measure of implied susceptibility. These actions alone do not contribute to the full comprehension of susceptibility, and have been studied in conjunction with other factors that influence levels of susceptibility.

When considering the role of personality traits, specifically the Five Factor Model, individuals scoring high on extroversion and openness to new experiences were found to be more vulnerable to phishing attacks (Hong et al., 2013). In the same study, individuals scoring high on introversion and individuals scoring low on openness to experience were more likely to delete legitimate emails, as opposed to phishing emails. Despite their increased vulnerability, Pattinson et al. (2012) showed that individuals scoring high on extroversion and openness to new experiences had knowledge of the appropriate actions to take upon receiving a phishing email. In their development of a framework to understand the relationship between personality traits and susceptibility to phishing attacks, Parrish et al. (2009) hypothesized that conscientiousness would be the personality trait most negatively associated with phishing, and agreeableness would be the personality trait most positively associated with phishing. The hypothesis on conscientiousness

has been supported in literature (Uebelacker & Quiel, 2014), as individuals with lower levels of conscientiousness are more willing to exchange their privacy for convenience. As for agreeableness, the results were mixed; individuals that scored high on agreeableness tended to be more susceptible to security risks (Darwish et al., 2012) but individuals who scored low on agreeableness also tended to engage in deviant workplace behaviors like breaking the rules of the organization, potentially making them more susceptible to social engineering attacks in that respect (Salgado, 2002). Individuals scoring high on neuroticism were found to be less susceptible to social engineering attacks, which can be attributed to their tendency to display more sensitivity over personal information disclosure and privacy issues surrounding it (Weirich & Sasse, 2001).

The relationship between personality traits and susceptibility to social engineering attacks can be explained by demographic variables as well. Research has consistently shown that females tend to be more susceptible to social engineering attacks compared to males (Darwish et al., 2012; Halevi et al., 2013; Hong et al., 2013, Uebelacker & Quiel, 2014). One of the reasons found for this disparity is the lower levels of technical experience that females tend to report compared to males (Sheng et al., 2010). Another explanation can be found in the differences in personality traits exhibited by both groups; research has shown that females tend to display higher levels of agreeableness compared to males, which potentially explains their increased susceptibility. However, it should be noted that outside of demographical analyses, little attention has been paid to the antecedents of why females are more susceptible than males to social engineering attacks. A meta-analysis of later studies conducted on susceptibility to social engineering attacks based on gender found that results were largely inconclusive, with no significant differences in gender groups on susceptibility to SE attacks (Montañez et al., 2020).

Other demographic-type variables that have been considered in the research of individuals' susceptibility to social engineering attacks are age and education, where education refers to the general education that individuals pursue post-graduation from high school. It is of note that across all papers surveyed for this research, no studies on social engineering studied populations younger than adults (less than eighteen years of age). This is most likely because research on social engineering attack susceptibility is undertaken with the assumption that the adult population is more likely to experience social engineering attack attempts, especially employees in organizations (Aldawood & Skinner, 2019). Regardless, age has been consistently found to be significantly associated with susceptibility to social engineering attacks, with younger individuals

between the ages of 18-25 being more susceptible to social engineering attacks compared to older individuals (Darwish et al., 2012; Sheng et al., 2012).

Aldawood and Skinner (2018) found trust in establishments and entities as an important element of assuring security and safeguarding individuals from social engineering attacks. When computer users are aware of the risks and threats that they can face in the online environment, including but not limited to social engineering attacks alone, their trust in entities can mediate self-security behaviors and protection from attacks. Along with trust, individuals with high self-awareness also tended to exhibit increased resistance to any attempts of social influence and persuasion attempts, which in turn made them less susceptible to social engineering attacks. However, this finding was largely context dependent, based on the powers and responsibilities of the individual, and the environment that they were in. For example, if the individual is aware that they are interacting with others in a highly deceptive environment, they would be less likely to disclose information about themselves, thereby reducing their susceptibility to any social engineering attacks that attempt to take advantage of their information (Williams et al., 2017).

While the aforementioned points of discussion provide a relatively comprehensive overview of the major factors that affect susceptibility to social engineering attacks, there are some limitations in general that make it difficult to extrapolate all results to the population. A lot of the studies referenced previously studied susceptibility to social engineering attacks in their samples by testing individual responses to attacks like phishing emails. Individuals were already notified that they would be taking part in a phishing experiment, which could explain some of the disparity in the consistency of results across groups. Individuals might also feel more motivated to accurately classify attacks, which implies a relatively imprecise representation of actual behaviors in online environments where individuals are not informed in advance of impending attacks. The samples used largely tended to be convenience samples, with focuses either in organizations or across university students in a specific area of study. Finally, all papers reviewed for this research were published over roughly two decades. In current times, awareness of social engineering threats may have potentially increased across all demographic groups so results from all studies may or may not apply to the current population of interest. Depending on privacy attitudes that individuals hold in contemporary times, knowledge of and experiences with social engineering attacks may have also increased.

2.3 Countermeasures against Social Engineering

Many solutions, both technological and psychological, have been developed and studied to tackle the increasing problem of social engineering attacks. Most solutions researched focused on the efficacy of behavioral changes across audits and specific scenarios, while other solutions studied were safeguards like spam filters and firewalls, and their effectiveness in preventing technical SE attacks (Parthy & Rajendran, 2019). For the scope of this research, solutions that are geared towards combatting human-based social engineering attacks are discussed.

Peltier (2006) focused on measures to bolster potential security breaches such as limiting access to restricted spaces, implementing password protection standards, and developing effective employee policies and procedures. The intervention that has been emphasized the most in research is user education on security awareness. Peltier (2006) argued that education of employees was vital in defending an organization against social engineering attacks, with a focus on encouraging the individual to value their role in the information security chain of the organization. Interventions in human behavior and user awareness have been studied across different groups and different environments, and have produced relatively consistent results. In their study, Bullée et al. (2015) found that subjecting an experimental group of university workers to an intervention about social engineering attacks decreased the susceptibility and compliance of the group to the subsequent social engineering attack executed by the researchers. The intervention provided information on what social engineering attacks were and the dangers of falling victim to such attacks, how to detect the attacks, and how to respond in such situations. The control group in this study was 2.84 times more likely to fall victim to the social engineering attacks, compared to the experimental group that received the education intervention. In line with educating individuals about social engineering attacks, Smith et al. (2013) studied the effectiveness of awareness websites and quizzes on individuals' understanding and avoidance of risks from social engineering attacks. Individuals were more likely to correctly identify phishing emails presented in quizzes after reading the educational material, compared to individuals that did not read the educational material. In terms of defenses against the psychological tactics employed in social engineering attacks, Schaab et al. (2017) proposed that more emphasis should be placed on tackling the persuasive principles that attackers use to manipulate their targets. Some types of solutions discussed included exposure to the persuasive tactics used by social engineers, attitude bolstering, and reality checks

for individuals so that they could understand the true extent to which they were vulnerable and therefore feel more motivated to defend themselves against social engineering attacks.

2.4 Defining Privacy in the Online Space

To understand the relationship between privacy and social engineering, it is important to understand the construct of privacy in the online space. Of the numerous definitions of privacy available in research, most definitions allude to privacy as a right of individuals to determine how much of their information can be shared and made available publicly. There is an element of decision and control associated with privacy, wherein the individual decides how much about themselves they share with others, and how much of that disclosed information they can restrict based on situations and preferences. This approach differs from the stance of viewing privacy as an interest, which in turn would change the definition of privacy and potentially the pertinence of assuring privacy (Tavani, 2008). In general, Westin (1967, as cited in Westin, 2003) defined privacy as the ability of the individual to decide how their information is communicated to others. This implies that the individual has the right to determine under what circumstances they share something about themselves, the extent of information that is shared, and the right to know how much of their information is shared or collected. A similar definition for information privacy, adapted from Westin (1967), was provided by Bergmann (2008), wherein information privacy was defined as the "right of self-determination regarding data disclosure". This was also supported by Zeissig et al. (2017), where the definition of online privacy was considered synonymous with information privacy. For this research, the definition of online privacy will also draw upon the definition of information privacy. Floridi (2005) posited that informational privacy is dynamic in the realm of information and communication technologies (ICTs); the increased use of ICTs fundamentally changes the extent to which information about individuals is disclosed. Therefore, information privacy in this context is achieved when individuals choose to restrict their information. Tavani (2008) posited that the relationship between computing/technology and personal privacy, and resulting concerns about information privacy pertaining to the individuals, could be analyzed through four main factors: the amount of personal information that could be collected about an individual, how quickly this information could be collected, the duration of retention of data, and the types of information that could be collected (Tavani, 2008, p. 139).

The fundamental concepts behind information privacy can be related to current discussions on privacy in the online environment. Continued advancements in information processing technologies have enabled numerous entities to collect and process large amounts and types of data associated with individuals. This in turn has led to discussions on online privacy and potential threats that people could encounter with respect to it. Nissenbaum (2011) argued that situational contexts determined the constraints on information disclosure. As such, an individual's understanding of privacy and subsequent information disclosure behaviors would be dependent on the online platform or service that individuals use, the perceived risks and benefits of using the specific platform or service, and the entities or groups of entities that the individual trusts.

In most research on privacy online, there is a lack of distinction between what constitutes privacy behaviors and security behaviors, and some of their antecedents respectively. This is because the concerns and attitudes that individuals tend to hold about their privacy and security tend to be similar, and limited research has been conducted on studying the differences between these two concepts across different contexts. With that said, some research suggests that while some facets of information privacy and security are similar, there are unique dimensions to security that differentiate it conceptually from privacy (Bansal, 2017). One of the definitions of information security is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability" (NIST, n.d.). The differences based on definitions lie in the goals behind assuring privacy and security respectively. Where privacy is largely concerned with restricting or limiting the amount of information about oneself that can be communicated or accessed, security largely deals with protecting information from manipulation or destruction in order to maintain the state and quality of data. However, there are some apparent overlaps in these two concepts; both privacy and security also consider the role of access to and disclosure of information. This discourse is relevant for the scope of this research because this overlap is apparent in the behaviors that individuals exhibit online to protect their privacy and security. This research will only address privacy concerns and behaviors in individuals but will be undertaken with the understanding that some privacy behaviors can likely be classified as security behaviors as well.

2.5 Factors Influencing Online Privacy

Numerous factors, demographic or otherwise, have been investigated to understand an individual's privacy concerns and behaviors in the online environment. Yao et al. (2007) found that at the time of their research, the levels of privacy concerns amongst surveyed experienced Internet users decreased over a period of four years. This was attributed to the level of familiarity with the internet; the more aware individuals were of privacy affordances and threats on the internet, the less they seemed to care about their online privacy. Other research studies yielded mixed results about privacy awareness on privacy concerns and behaviors. In a review of the relationship between demographic groups and online privacy concerns, O'Neil (2001) found that all demographic groups (sexes, education levels, income levels, and ethnicities) preferred maintaining their online privacy to any conveniences that online services would offer. However, this finding is not supported in later research. In their study of online privacy in social media, Debatin et al. (2009) found that while individuals indicated that they were aware of the different privacy issues associated with social media accounts, they still intended on using social media applications due to the benefits outweighing the risks associated with the issues. Individuals also allowed large groups of people online to view personal information available on their online profiles, despite any privacy concerns they might have held. Similarly, Nyoni and Velempini (2018) found that users of social media regularly post personal information on their online profiles despite threats to privacy. They also found that most users did not understand the affordances available to protect their personal data online. Barth et al. (2019) found that individuals tended to care more about the convenience and benefits associated with applications rather than their personal privacy.

Trust in entities has also been investigated to understand people's attitudes about their online privacy. Pötzsch (2003) found that individuals were less concerned about their privacy online if they had established trust in the entities who were the perceived recipients of their information. This finding was also supported by Bergström (2015), who found that trust in other people was the most important factor explaining the online privacy concerns that individuals had. If individuals trusted others who had access or ownership of their personal information, they were less concerned about the misuse of their personal information. However, in doing so, individuals may not realize that the entities they consider trustworthy may not be the only entity with access to their data (Pötzsch, 2003). In their survey of online privacy concerns amongst older adults, Zeissig et al. (2017) found no significant differences in levels of trust reported by different age

groups but reported that young adults had the highest trust in online companies, while middle-aged adults had the lowest trust in online companies.

Another factor that has been studied in the literature on online privacy is the level of education or knowledge that an individual has about technology and the internet. This is slightly different from traditional education, in that it considers the literacy and familiarity of the user with the online environment. Malandrino et al. (2013) found that individuals who pursued education in majors related to information and communication technology (ICT) were less concerned about their online privacy compared to individuals who pursued education in other areas. The general implication from this finding was that individuals who were more educated about technology overall had fewer concerns about their privacy owing to their comprehension of risks to privacy. With that said, the study also found that across all groups, individuals did care about their privacy but did not significantly partake in any behaviors to effectively protect it. However, Bartsch and Dienlin (2016) found that individuals with greater online privacy literacy engaged in more privacy protective behaviors online. In this study, privacy literacy was also studied in relation to the amount of time that individuals spent online, suggesting that the more time a person spent on the Internet, the more familiar the individual would be with privacy risks and threats they could potentially face across different online environments. Barth et al. (2019) found that despite awareness of privacy risks, technically skilled individuals still continued to use online applications that could pose potential risks to privacy. The findings on the relationship of technology education and knowledge on privacy concerns and behaviors are somewhat mixed but still suggest that some levels of awareness can enable individuals to partake in protective behaviors or at the very least, understand and use the affordances provided to protect access to their information online.

With that said, the effect of regular education on privacy concerns and behaviors has been largely consistent throughout the literature. Individuals with higher levels of education were found to be more concerned about their privacy online and were also reported to engage in more privacy protective behaviors (Cho et al., 2009; Hazari & Brown, 2013; Milne et al. 2004; Sheehan, 2002). However, O'Neil (2001) found that levels of education did not significantly affect individuals' online privacy concerns, and Boerman et al. (2018) found that education did not predict changes in privacy protective behaviors. Overall, when considering the role of both general and specialized education, effects on online privacy concerns and on engagement in protective behaviors are mixed. It is worth mentioning that in most of the studies discussed, education was studied along with other

factors like demographic groups (more of which will be discussed later in this section), but the results pertaining to education were obtained separately and not in conjunction with any other factors that were being investigated in these studies.

Demographic variables like age, gender, and ethnicity have also been investigated to understand if such differences can affect the perceptions of privacy that individuals have, and the behaviors that they engage in as a result. Studies on the effect of gender so far have yielded mixed results. Some studies have contended that women express higher privacy concerns than men (Cho et al. 2009, O'Neil, 2001). However, there is evidence that men were more likely to express higher privacy concerns than women and engage in privacy protective behaviors (Milne et al. 2004). Most studies that consider the effect of demographics found no significant effects of gender on privacy concerns (Boerman et al., 2018, Hazari & Brown, 2013, Yao et al., 2007). With that said, Yao et al. (2007) found that women reported lower levels of internet usage, technology fluency, and self-efficacy, suggesting that while there are no significant impacts of gender on privacy concerns, there still exists a disparity in usage that cannot fully capture all concerns that different groups might have.

The findings related to age are also mixed. Age has long been considered a variable of interest due to the differences in the adoption of technology and the use of online services across different generations. In their research on classifying internet users based on levels of privacy concern, Sheehan (2002) found that most Internet users who were either "unconcerned" or "alarmed" about their privacy tended to be middle-aged (between 45-54 years of age), compared to users in other groups. The major implication from this study was that understanding online privacy through age-based groups would be complicated due to the contextual nature of privacy, and this finding has been largely reflected in subsequent research on the effects of age. Zeissig et al. (2017) found that older internet users reported higher levels of privacy concerns compared to younger internet users, but the differences were not significant. Regardless, older adults were found to significantly exhibit higher levels of privacy protective behaviors compared to other age groups. On the other hand, Milne et al. (2004) found that age was inversely related to engagement in privacy protective behaviors, suggesting that younger adults were more likely to exhibit privacy protective behaviors than older adults. Other studies have found that age is not a significant predictor of privacy concerns or behaviors (Boerman et al., 2018, Hazari & Brown, 2013).

Other demographic variables have been studied limitedly in literature. For instance, Hazari and Brown (2013) found that employment status was significantly related to the reported privacy knowledge of individuals, but was not a significant predictor of privacy concerns and behaviors. O'Neil (2001) found that individuals with higher income levels tended to be less concerned about their online privacy compared to individuals with lower income levels. There is limited research on the relationship between online privacy and reported ethnicities. It has been hypothesized that cultural dimensions and differences could affect people's perceptions of rights to privacy and opinions about the efficacy of privacy behaviors, and this is reflected in minimal research on the same.

There is evidence to indicate that there are some group differences across ethnicities in the perception of privacy concern; in one study, across different ethnicities in the United States, Caucasians and Asians/Pacific Islanders reported the lowest levels of privacy concerns, while Latinos/Hispanics reported the highest levels of privacy concerns (O'Neil, 2001). Perceptions of privacy and privacy protection vary across different countries as well. Orito et al. (2008), in their research of online privacy perceptions, knowledge, and behaviors in Japan, found that despite the majority of respondents reporting a limited understanding of the "right to privacy" itself, individuals largely agreed on the importance of protecting their privacy and valued their personal information highly across online environments. Similarly, Cullen (2009) found that information privacy concerns varied between New Zealander and Japanese ethnic groups, with New Zealander groups reporting higher privacy concerns about their personal information online compared to the Japanese groups. This was attributed to the extent of technology use across both countries.

Online privacy is also influenced by negative experiences that individuals have online. The effects of this have been studied limitedly in research, at least when considering it from the perspective of general privacy concerns and behaviors. Cho et al. (2009) found that individuals who reported experiences of privacy invasion, like receiving spam emails, were more likely to have higher levels of online privacy concerns. This finding was somewhat supported by Chen et al. (2017), where they found that individuals who were victims of internet scams had increased online privacy concerns. This in turn significantly predicted the engagement of these individuals in privacy protective behaviors.

Overall, online privacy concerns and behaviors can be influenced by a lot of internal and external factors relating to the individual. Some findings contend that individuals care about their

online privacy and engage in behaviors to protect it when personal information is at stake. However, when considering the benefits gained from utilizing online platforms and services, and the convenience associated with such things, concerns about online privacy can be diminished or disregarded altogether. This in turn implies lesser engagement in privacy protective behaviors.

2.6 The Relationship between Social Engineering and Privacy

As discussed in earlier sections, social engineering attacks that target people may or may not require attackers to possess sufficient knowledge and background about their targets. Depending on the types and magnitude of attacks that are launched, attackers might need to possess some amount of background knowledge about their targets. For instance, spear-phishing attacks require attackers to collect as much information about their victims as possible (Salahdine & Kaabouch, 2019). This knowledge can be obtained from a variety of sources but is most often solicited through indirect means such as intelligence gathering from public sources. This is related to online privacy as attackers can take advantage of individuals' notions about privacy (or lack thereof) in numerous ways. Based on how people online allow their friends or the public to view their information on different online networks (Debatin et al., 2009), attackers can launch pretexting attacks based on publicly available information. This helps the attackers gain the trust of unsuspecting individuals and use their information against them for malicious purposes. Social engineering attacks are detrimental to the privacy of the individual, especially attacks that attempt to elicit sensitive information from people.

Research on the relationship between social engineering and privacy, particularly from the perspective of privacy needs and behaviors as a deterrent to social engineering attacks, is severely limited. Orgill et al. (2004) argued for the need for privacy education to counter social engineering attacks, as opposed to focusing on security behaviors alone. Gürses (2014) contended that with increased data breaches in corporations and large entities, and inadvertent compromise of personal information by individuals, there would be a need for professionals to build "privacy solutions" into systems. This is largely seen in practice today with technical measures to combat privacy and security issues being implemented into systems, but it still does not fully account for the variety in individual attitudes to privacy and subsequent actions that individuals might take to protect their privacy. Developing new affordances and enhancing older ones is useful given the dynamic nature of the internet and flow of information, but these affordances would be rendered useless if not

utilized properly by individuals. To this end, it is imperative to think about the antecedents in the development of privacy protective behaviors in individuals, and how those behaviors could help mitigate the susceptibility of individuals to social engineering attacks. To the best of current knowledge, this research would be novel in its approach of understanding susceptibility to social engineering attacks through the inherent dispositions people hold about privacy and subsequently developed protective behaviors as a result. Apart from the inherent need for privacy, other insights from behavioral theories can also be used to understand what drives individuals to develop privacy protective behaviors, more of which will be discussed in the following section.

2.7 Theoretical Framework

Many theories have been used to understand the behaviors of individuals in relation to online privacy. Application of the theories differs depending on the online situation or context that privacy is being studied in. Li (2012) identified numerous theories used in online information privacy research, the most popular of which were privacy calculus theory, expectancy-value theory, social contract theory, and theory of reasoned action. Privacy calculus theory posits that an individual's intention to disclose their information would be based on a "calculus of behavior". This calculus involves individuals weighing competing factors against possible outcomes and making decisions about information disclosure based on a risk-benefit analysis (Dinev & Hart, 2006). Expectancy-value theory posts that motivation and subsequent behaviors in individuals can be determined by expectancy, which is the extent to which individuals believe that they can control or influence outcomes, and value, which is the amount of importance and utility that is assigned to the task (Wigfield & Eccles, 2000). Social contract theory, within the context of information privacy research, suggests that social contracts oversee the relationships between individuals and entities with respect to information disclosure across online environments. These social contracts involve the establishment of agreements between individuals and entities, and these agreements or "contracts" govern the behaviors of all parties in information exchanges (Faja & Trimi, 2006). The theory of reasoned action posits that an individual's behavior is determined by their intention to actually engage in the behavior. This intention is influenced by any attitudes that are held about the specific behaviors, and the subjective norms surrounding the individual (Sheppard et al., 1988).

The development of privacy protective behaviors against SE attacks can be attributed to the motivation that the individual develops to engage in such behaviors. This research study drew

upon elements of protection motivation theory (PMT) in addition with other individual factors like the psychological need for privacy and past experiences with social engineering attacks, operationalized by falling victim to these attacks. PMT was chosen for this study due to the applications of the theory in information security research, particularly with respect to engaging in behaviors that could protect individuals from perceived threats to their privacy and security online. The following sections cover the use of PMT in information privacy and security research, and the applications of the psychological need for privacy in the same.

2.7.1 Protection Motivation Theory

Protection motivation theory (PMT) was first proposed as a theory of health psychology by Rogers in 1975 to understand an individual's motivation to change their behaviors based on fear appeals. The basic premise of the theory is understanding how messaging aimed at fears about certain habits can initiate behavioral changes about those habits. The original postulates of PMT contended that there were three crucial components of a fear appeal – the magnitude of noxiousness or harm, the likelihood of occurrence of the threat, and the efficacy of the response against the threat (Rogers, 1975).

A revision to the theory in 1983 included the addition of the theory of self-efficacy alongside response efficacy, and the components combined were found to be significant predictors of behavioral intentions, with self-efficacy being the most powerful (Maddux & Rogers, 1983). PMT posits that an individual's motivation to change their behaviors depends on the cognitive threat appraisals and coping appraisals that the individuals develop in response to perceived threats. Threat appraisals consist of the perceived severity from the threat and the perceived probability of the threat affecting the individual. Coping appraisals consist of the self-efficacy of the individual in committing the preventative behavior, and the efficacy of the preventative behavior itself, which is also known as the response efficacy. When threat and coping appraisals are high, individuals are highly motivated to engage in protective behaviors against the perceived threats.

PMT was initially used extensively to understand the effects of fear appeals on predicting and changing health behaviors (Norman et al., 2005). In recent times, applications of PMT have been found in information security, particularly in the realm of privacy concerns, security behaviors and awareness campaigns. Studies have used all or some of the factors from the original

PMT model. In their meta-analysis of 30 selected studies using PMT to understand information security behaviors, Sommestad et al. (2015) found that PMT can be used to explain information security behaviors if the threat and coping appraisals are explicitly stated in measures (i.e., the threats to security are clearly identified, and individual or types of coping behaviors are properly stated), and if the threats relate to the individual instead of the organization or entity that the individual might be a part of. In another study, individuals who exhibited higher levels of threat appraisals were more likely to actually comply with information security policies, implied to be protective in nature (Siponen et al., 2006). Yoon et al. (2012) found that individuals with high levels of response efficacy and self-efficacy exhibited higher intentions to practice information security behaviors, which in turn predicted actual engagement in those behaviors. Crossler and Bélanger (2014) found that the four main factors comprising the threat and coping appraisals in individuals were significantly related to engagement in security protective practices, and explained most of the variance in individual security practices.

Salleh et al. (2012) found significant relationships between all factors in the PMT model to privacy concerns. Boerman et al. (2018) found that of all the factors in the PMT model, perceived severity and response efficacy had significant small positive effects on privacy protective behaviors. Similarly, in their study on the application of PMT to understand privacy concerns, Mousavizadeh and Kim (2015) found significant positive effects of perceived susceptibility and severity on privacy concern and subsequent motivation, and significant negative effect of response efficacy on privacy concerns. Zeissig et al. (2017) found that privacy self-efficacy of individuals was a significant predictor of engaging in protective behaviors, which supports Maddux and Rogers (1983) finding of self-efficacy being a significant predictor. However, this is not consistent across research as other studies found self-efficacy a non-significant predictor of protective behaviors (Boerman et al. 2018, Mousavizadeh & Kim, 2015).

Overall, there is good support for the use of PMT in understanding privacy and security behaviors, but there are some limitations with these studies. Across studies, the variables of PMT explain anywhere from 30% to 39% of the variance in information security behaviors (Crossler & Bélanger, 2014; Yoon et al., 2012), suggesting that additional variance can be explained by other factors in conjunction with the PMT constructs. Studies using PMT also tend to focus more on intentions to engage in protective behaviors rather than measurement of the actual engagement in the behaviors itself (Sommestad et al., 2015).

2.7.2 The Psychological Need for Privacy

According to the Encyclopedia of Individual and Personality Differences, the need for privacy is defined as the "need to selectively control the access of others to the individual self with the aim of achieving a desired level of physical or psychological privacy" (Trepte & Masur, 2020, p. 3132). This is considered analogous to maintaining a form of solitude or reserve. The need is manifested from an individual's motivation to control aspects of their personal information disclosure, which would fall in line with definitions of privacy in terms of considering its purpose (Bergmann, 2008; Westin, 1967). Trepte and Masur (2020) further posited that the need for privacy is a secondary need for individuals, as fulfilling the need for privacy could help individuals attain other fundamental goals.

Like privacy concerns, the need for privacy does not manifest in online environments alone. The need is dynamic based on the situational contexts and general individual differences. For the most part, individuals tend to have strong motivations to protect their privacy, but the extent of these motivations vary (Krämer & Schäwel, 2020). Studies on the need for privacy have focused on different areas like the variation in need for privacy across longitudinal contexts and sociocultural contexts, as well as individual personality differences (Trepte & Masur, 2020). Dienlin and Metzger (2019) found that individuals who were less sociable were significantly more likely to report greater need for privacy across the studied dimensions of privacy from government and privacy from other people.

In the online space, the need for privacy has been studied in conjunction with information disclosure behaviors online, albeit limitedly. Babula et al. (2017) found that individuals were significantly less likely to disclose their data in experimental conditions after being subject to priming effects, thereby encouraging adherence to individual privacy expectations and standards. Blachnio et al. (2016) found that high scores on the measure of need for privacy significantly predicted lower usage of social media. This indicates that individuals who valued their personal privacy were less likely to disclose information about themselves on their online profiles. This is in line with prior findings about the need for privacy and online privacy concerns, where individuals who scored high on the need for privacy were found to have higher perceived control over their personal information and higher levels of online privacy concerns (Yao et al., 2007).

2.8 Research Model

Privacy concerns held by individuals, and the behaviors that they engage in as a result of these concerns, have been found to be influenced by numerous factors as discussed in the literature review, but limited findings are present on the effect of the psychological need for privacy on the adoption of privacy protective behaviors. There is support in literature for the need for privacy influencing the extent of personal information someone chooses to disclose about themselves. This is relevant for bolstering individual defenses against social engineering attacks as the inherent need for privacy that an individual possesses would help the person gauge the threat to their privacy by means of social engineering attacks, and subsequently enable the individual to engage in protective behaviors. Effective privacy education can bring attention to any contrary privacy or security behaviors, which implies an emphasis on the development and adoption of personal privacy protective behaviors as opposed to relying on external entities to assure privacy (Orgill et al., 2004). This in turn would help ensure that individuals are better prepared to identify and defend themselves against social engineering attacks, not only in workplaces but across all online platforms that the individual maintains a presence on.

The research model presented (see Figure 2.1) provides an overview of the relationships investigated in this study. The psychological need for privacy and social engineering victimization are specific factors that are hypothesized to have an impact on the extent of privacy protective behaviors that individuals engage in.

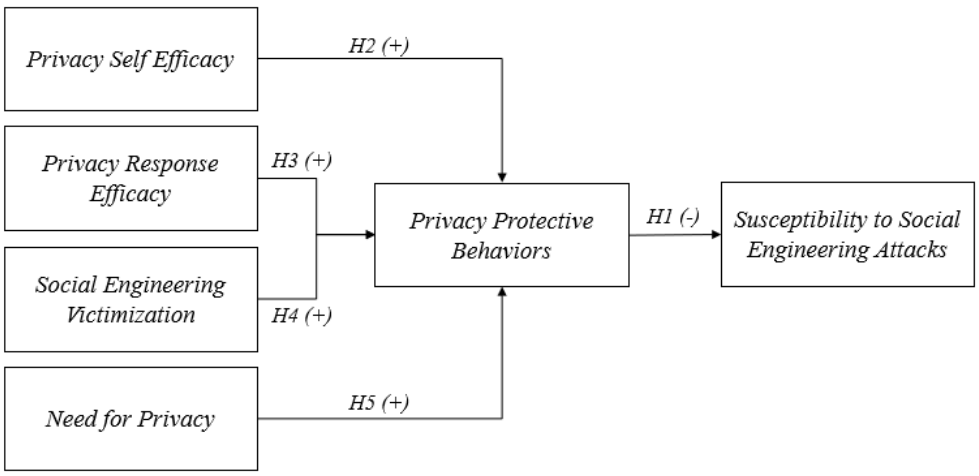


Figure 2.1 Research Model

The research model also considered the role of coping appraisals that individuals develop in response to threats from social engineering attacks. Rogers (1975) found self-efficacy to be the best predictor of behavioral intentions in people. This was eventually supported in information security research, where it was found that individuals with high levels of response efficacy and self-efficacy exhibited higher intentions to practice information security behaviors, which in turn predicted actual engagement in those behaviors (Yoon et al., 2012).

Due to the scope of the research, the model will only consider online privacy behaviors, as opposed to both privacy and security behaviors. Considering the overlap in privacy and security behaviors (Bansal, 2017) and similarities in measures of privacy and security behaviors (Pirim et al., 2008), some security behaviors will inevitably be included as privacy behaviors in this study. There are little to no findings on the role of privacy protective behaviors on susceptibility to social engineering attacks, but education and awareness of social engineering attacks has been long touted as an effective safeguard (Peltier, 2006). The limitation with this contention is that there is an unclear delineation of the type of education that people should receive (i.e., focus on theoretical knowledge versus procedural knowledge). Therefore, this study will consider the role of self-reported procedural knowledge, particular privacy protective behaviors that individuals already engage in, to understand the impacts of existing protective behaviors in defending against social engineering attacks. Operationally, privacy protective behaviors refer to the specific actions that individuals take across technology-based environments to assure the safety of their information. This operational definition is adapted from Boerman et al. (2018). The main hypothesis of this study was that individuals who engage in privacy protective behaviors will be less susceptible to social engineering attacks.

H1: Individuals who engage in privacy protective behaviors are less susceptible to social engineering attacks.

An implicit assumption that was made in this research model is that individuals readily perceive the threat of social engineering attacks. According to the 2016 Social Engineering Report, 60% of respondents perceived social engineering to be a significant threat, and indicated that they were victims of social engineering attacks (Abass, 2018). As a result, in the face of increasing SE

attacks, individuals would have to consider their self-efficacy with respect to assuring their privacy. The definition of privacy self-efficacy in the context of this study was adapted from the operationalization of the measure provided by LaRose and Rifon (2007), and refers to an individual's perceived capability of maintaining their online privacy. Therefore, based on findings in the literature review (Zeissig et al., 2017) it was hypothesized that individuals who score high on privacy self-efficacy are more likely to engage in privacy protective behaviors.

H2: Individuals who score high on privacy self-efficacy are more likely to engage in privacy protective behaviors.

The self-efficacy of the individual with respect to assuring their privacy is also related to the effectiveness of the privacy affordances (i.e., responses that are countermeasures to the threat) available to them. Individuals can be confident in the usefulness of their behaviors only if they perceive the existing responses to be effective against the threats social engineering attacks pose to their privacy. Response efficacy pertaining to privacy in this model was operationally defined as the extent to which individuals believe that popular protective measures can protect their online privacy. While results about the effect of response efficacy in literature is limited, based on the most relevant findings (Boerman et al., 2018), it was hypothesized that individuals who score high on the measure of response efficacy are more likely to engage in privacy protective behaviors.

H3: Individuals who score high on privacy response efficacy are more likely to engage in privacy protective behaviors.

Based on the literature review, individuals that reported past experiences with social engineering attacks were more concerned about maintaining their online privacy, and these concerns significantly predicted privacy protective behaviors in individuals (Chen et al., 2017; Cho et al., 2009). Therefore, it was hypothesized that individuals who have been victims of social engineering attacks in the past are more likely to engage in privacy protective behaviors.

H4: Individuals who have been victims of social engineering attacks are more likely to engage in privacy protective behaviors.

Compared to other studies on privacy protective behaviors, this study considers the role of the psychological need for privacy as a factor that influences engagement in privacy protective behaviors. The literature on the subject already suggests that a higher need for privacy is significantly related to greater online privacy concerns (Yao et al., 2007). The need for privacy in the context of this model is defined as the extent to which individuals desire control over the disclosure of their personal or sensitive information in online settings. A meta-analysis of literature on privacy concerns found that individuals who reported high levels of privacy concerns were more likely to engage in high levels of privacy protective behaviors (Baruh et al., 2017). A point of note here is that the same meta-analysis found no significant differences between studies that investigated behavioral intentions and studies that asked respondents to report their privacy protective behaviors. Therefore, it is hypothesized that individuals reporting a higher need for privacy will be more likely to engage in privacy protective behaviors.

H5: Individuals who score high on the need for privacy are more likely to engage in privacy protective behaviors.

To account for group differences based on demographics, the demographic variables were to be controlled for when studying the relationships between privacy protective behaviors and the independent variables that they were associated with. The demographics were also to be controlled for when studying the relationship between the privacy protective behaviors and susceptibility to social engineering attacks, based on evidence from the section discussing the relationship between privacy and social engineering.

CHAPTER 3. METHODOLOGY

The methodology section provides an overview of the research design that was developed and used for this study. This included identifying the relevant population and sample, as well as all the measures adapted or used for the independent and dependent variables of interest. This was followed by a discussion of the reliability and validity of these measures, and tests for the reliability and validity of the developed measure.

3.1 Research Design

The overarching research question that this study sought to answer is – does engagement in privacy protective behaviors mediate the relationship between specific privacy antecedents and susceptibility to social engineering attacks? To answer this question, the variables of interest and their measures were identified and hypotheses were drawn in the previous chapter. The mode of data collection used for this study was a survey. The survey was developed in Qualtrics, and distributed via Amazon Mechanical Turk (MTurk). Qualtrics is a web-based survey creation tool which allows for the collection and analysis of data (Purdue University, n.d.). Access to Qualtrics was provided through Purdue University. Amazon Mechanical Turk (MTurk) is a "crowdsourcing marketplace" that allows for people to crowdsource tasks and jobs to a distributed workforce (Amazon, n.d.). MTurk has been largely adopted in quantitative research due to the convenience with which researchers can gain responses from a broader audience. MTurk also offers researchers an efficient, cost-effective way of gaining responses from a relatively more diverse sample (Rouse, 2015). While the use of MTurk has increased across different areas of research, there still remain doubts about the reliability and validity of the data gained from this service (Aguinis et al., 2020). With these considerations in mind, potential issues to reliability and validity of the data are addressed in the following sections, and solutions or mitigations were included in the survey design. The research survey developed for this study was evaluated by the Institutional Research Board at Purdue University, and approved as IRB #2021-1042.

3.2 Population and Sample

The population identified for this study was all adults (i.e., individuals over the age of 18) who live in the United States. The sample comprised all adult MTurk users who live in the United States. There were no restrictions on the gender, ethnicity or education level of individuals. Based on Cohen's power tables, at 80% power and significance level of 2.5% (α = .025) the appropriate number of individuals to sample to detect a medium effect size would be approximately 200 people (Cohen, 2013). However, this was a general estimation and could change depending on the statistical tests that are conducted (Cohen, 1992). In order to account for attrition rates and invalid responses for this study, the proposed number of individuals to be sampled was approximately 250-300 individuals. The final number of preliminary responses received was 296, and of these, 272 responses were retained for analysis. Further details on data screening and retention of valid responses can be found in the next chapter.

3.3 Measures of Variables

Based on the research model, the variables were measured through a mix of researcher-developed questions and existing, validated instruments. The variables of interest for hypotheses testing were social engineering victimization (sometimes also referred to as SE victimization), the need for privacy, privacy self-efficacy, privacy response-efficacy, privacy protective behaviors, and the actual susceptibility to social engineering attacks. The demographic variables of age, gender, education and ethnicity were also treated as independent variables for preliminary analysis, and were controlled for if needed to understand the predictive utility of the independent variables uniquely on the dependent variables. All questions and measures developed for the survey are provided in the appendix of this thesis.

3.3.1 Measures of Demographic Variables

Individuals were asked to report their age by selecting one of multiple options representing different age ranges, with restrictions applied on the overall range to ensure that only adults would be taking the survey. Standard options for gender were used in the survey ("male", "female", "non-binary", "prefer not to say"). The options for reporting ethnicity were adapted from the United States Census Bureau standards on collecting data about race and ethnicity (US Census Bureau,

2020). Standard options for education were used in the survey, from reporting limited levels of schooling to advanced degrees at the university level.

3.3.2 Measure of Social Engineering Victimization

Social engineering victimization in the context of this study refers to whether an individual had fallen for a social engineering attack. This was gauged by two questions. Individuals were asked if they had been a victim of social engineering attacks, and if they had suffered serious consequences as a result of the attack(s). These questions were framed based on prior findings about the relationship between past experiences and susceptibility to social engineering attacks. In their meta-analysis of studies on the impacts of past experiences, Montañez et al. (2020) found that individuals who fell victim to social engineering attacks in the past were less susceptible to present attacks, particularly those individuals who experienced significant losses from past SE attacks. The options provided for the question on social engineering victimization were intentionally delimited to the three most common attacks reported to the IC3 in the past year: phishing, smishing and pharming. The definitions provided for the three types of attacks were based on Salahdine and Kaabouch (2019). Based on whether an individual was a victim of one or more social engineering attacks, the variable was recoded into "SE_Victimization", a dichotomous variable that indicated whether an individual was a victim or non-victim of a social engineering attack, regardless of how many attacks they indicated they were a victim of. The counts of victimization for the three types of attacks were also retained.

3.3.3 Measure of Need for Privacy

Multiple measures have been developed to understand the need for privacy in individuals (Buss, 2001; Pirim et al., 2008; Yao et al., 2007). For the scope of this research, the need for privacy measure developed by Trepte and Masur (2017) was used as it was created to investigate the need for privacy separately from the need for security. More notably, Trepte and Masur (2020) also provided an overview of the widely accepted definition for the psychological need for privacy that is established in the Encyclopedia of Individual and Personality Differences. The perceived need for privacy instrument consists of twelve items measuring privacy with respect to control over the communication of and access to personal information about oneself across online and

offline environments. The items were measured on a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). The reliability analysis for this scale from the original study indicated that the scale had good reliability (Cronbach's α = .81). An example of a question from the scale is: "I do not want my personal data to be publicly available". The average score of all the items on the scale would indicate the individual's need for privacy. Reliability analyses on the items of this scale in this study indicated that the scale had good reliability (Cronbach's α = .84).

3.3.4 Measure of Privacy Self-Efficacy

The measure of privacy self-efficacy was used from Zeissig et al. (2017). This scale was developed to understand the confidence that individuals have in protecting themselves online through their privacy settings in general online platforms. The measure consists of six items and was measured on a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). The reliability analysis for this scale in the study indicated that the scale had acceptable reliability (Cronbach's α = .69). An example of a question from the scale is: "I always change my privacy settings when I start using a new application". The average score computed from the items on the measure constitutes the level of privacy-self efficacy an individual has, with a lower score indicating a higher level of privacy self-efficacy. The privacy-self efficacy scale cited from Zeissig et al. (2017) has a lower value of internal consistency. The researchers justified the use of the scale by using a benchmark of $\alpha > .60$ for the acceptance of reliability of the measure, particularly due to the exploratory nature of operationalizing privacy self-efficacy, as opposed to general self-efficacy that is presented in the PMT model. Some research suggests that a value of .60 to .70 would indicate an acceptable level of reliability, and values above .60 would indicate an acceptable level of reliability (Ursachi et al., 2015). Therefore, the privacy self-efficacy scale was retained for preliminary analysis. The reliability analysis conducted for this study indicated that the scale had marginally acceptable reliability (Cronbach's α = .66).

3.3.5 Measure of Privacy Response Efficacy

The measure of privacy response efficacy was used from Boerman et al. (2018). This scale consists of 9 items related to privacy protective measures. Individuals were asked to indicate whether specific protective measures would be effective against misuse of personal information,

which in turn was related to assuring their privacy online. The items in Boerman et al. (2018) were measured on a 7-point Likert scale (1 = Strongly Disagree, 7 = Strongly Agree). The reliability analysis for this scale in the original study indicated that the scale had good reliability (Cronbach's $\alpha = .93$). An example of a question from the scale is: "Please indicate the extent to which you agree with the following protective behaviors being effective against collection, usage and sharing of personal information on the internet: Deleting Cookies". The average score of all items on the scale was computed to determine the level of privacy response efficacy held by an individual. The reliability analysis conducted for this study indicated that the scale had good reliability (Cronbach's $\alpha = .82$).

3.3.6 Measure of Privacy Protective Behaviors

The measure of privacy protective behaviors was also adapted from Boerman et al. (2018). The scale used by Boerman et al. (2018) asked individuals to indicate how often they engaged in ten specific privacy protective behaviors. The options provided were never, rarely, occasionally, often, very often, and do not know. The reliability analysis in their study indicated that the scale had good reliability (Cronbach's $\alpha = .82$). For this research, this 10-item scale will be used but additional privacy protective behaviors were added to the measure based on recommendations from cybersecurity organizations and research. An example of a question from the scale is: "How often do you use a virtual private network (VPN)?" The final measure consisted of 12 items, as some recommendations were already incorporated into the original scale. Based on the recommendation from the developers of the scale, the option of "do not know" was recoded as a missing value. The remained of the options were assigned a value from one to five (1 = Never, Very Often = 5). The average score of the items on this scale was used to determine the level of engagement in privacy protective behaviors. The reliability analysis conducted on the 12-item scale indicated that the scale had good reliability (Cronbach's $\alpha = .82$).

3.3.7 Measure of Susceptibility to SE Attacks

The measure of susceptibility to SE attacks was adapted from studies that have investigated the susceptibility of individuals to specific attacks like phishing. For instance, Hong et al. (2013) empirically measured susceptibility among study subjects by asking them to classify a set of emails

as phishing, spam, malware or legitimate emails. Halevi et al. (2013) measured susceptibility to SE attacks by sending phishing emails to survey participants and counting the number of individuals who clicked a field within the malicious link sent in the phishing email. Based on the approaches used in these studies, this research study also presented scenarios to individuals. What distinguishes this study from others is the focus on the top three types of social engineering attacks that were reported to the FBI in the past year – phishing, smishing and pharming attacks (Internet Crime Complaint Center, 2021). This is a relatively unique contribution to the body of knowledge on understanding susceptibility to SE attacks, particularly as most studies tended to focus on susceptibility to phishing emails alone.

For this study, respondents were presented with a total of 21 scenarios, divided across three modes of communication – emails, text messages and websites. The scenarios overall consisted of a mix of legitimate communications and social engineering attacks, and individuals had to indicate how confident they were about classifying a scenario as a social engineering attack. This was measured on a 5-point Likert scale (1 = Not at all confident, 5 = Extremely confident). Figure 3.1 represents an example of a social engineering scenario and Figure 3.2 represents an example of a legitimate scenario. Some of the scenarios in the survey were obtained from public cybersecurity sources on the Internet, and the rest of the scenarios (legitimate and social engineering attempts alike) were provided from the researcher's personal communications. All scenarios used for the survey are provided in the appendix. The average scores of all the items in this scale constituted the overall susceptibility score for the individual. The reliability and validity analysis conducted over the scale items are discussed in a later section.

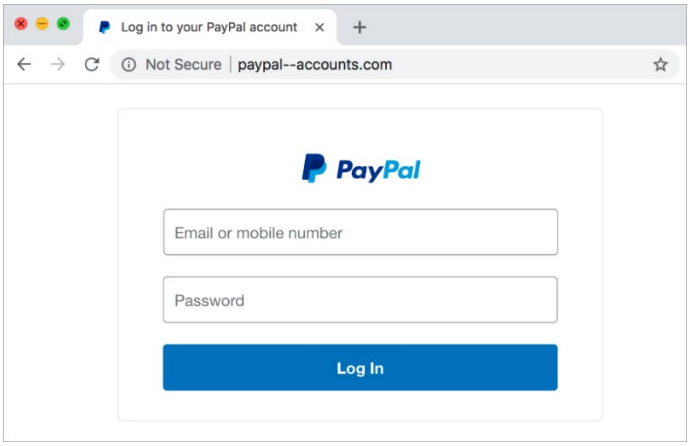


Figure 3.1 Example of a Social Engineering Scenario

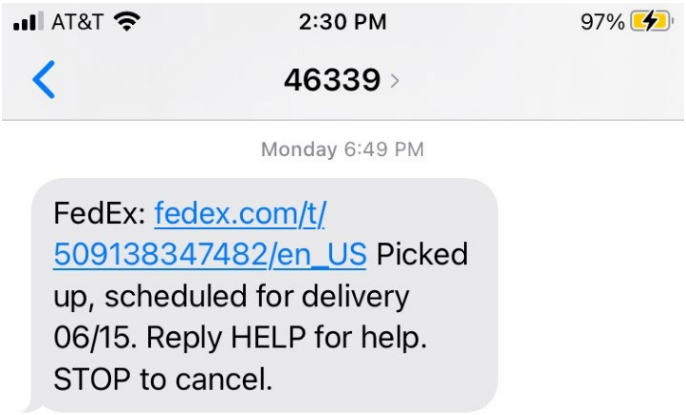


Figure 3.2 Example of a Legitimate Scenario

3.4 Validity and Reliability of Adapted Measures

In this section, the threats to the reliability and validity of the measures are discussed. The reliability of a measure refers to the consistency of the measure in measuring a construct. It refers to whether the measure produces the same results when used across time, evaluated for all items in the measure, and when used by different researchers (Price et al., 2015). For all the measures discussed in the previous section, the internal consistency of all measures was computed through statistical reliability analyses in their respective studies. A value of .80 is generally considered to represent good internal consistency (Price et al., 2015). Therefore, almost all measures used in this study were purported to have good internal consistency. The development of the measure for privacy self-efficacy was guided by PMT, but the measure itself does not meet the threshold for good internal consistency according to Price et al. (2015). However, the value of Cronbach's alpha is also impacted by the number of items in the scale. The value of alpha can be reduced if there are fewer items on the scale (Tavakol & Dennick, 2011). The relatively low value for the privacy self-efficacy measure can be attributed to the number of items in the scale. As discussed before, due to the exploratory nature of the study and the development of the privacy self-efficacy scale as a construct specific to understanding efficacy related only to online privacy, the measure was retained.

Inter-rater reliability for all the measures was not explicitly measured as there was only one researcher primarily working on the project and collecting all proposed data, but potential bias from this researcher was addressed through the anonymization of data collection. Finally, the test-

retest reliability of all the measures were partly evaluated through implementation in this study, and partly through investigating the use of the measures in other studies. To the best of current knowledge, the need for privacy measure developed by Trepte and Masur (2017) and the privacy self-efficacy measure developed by Zeissig et al. (2017) have not been used in other studies. Some items from measure of privacy protective behaviors developed by Boerman et al. (2018) has been used in conjunction with other items measuring privacy protective behaviors, and the measure of the combined items also has good reliability (Cronbach's α = .85) (Kruikemeier et al., 2020).

The validity of a measure refers to the extent to which the measure actually represents the construct that it is measuring (Price et al., 2015). The content validity of all the measures can be assessed by evaluating the development of the measures themselves. The perceived need for privacy scale developed by Trepte and Masur (2017) was part of a larger study to accurately assess an individual's perceived need for privacy across a sample that was representative of the population of interest. The items on the perceived need for privacy scale were created based on past research about control over the dissemination of private information. The study itself was part of a five-wave, longitudinal research project conducted over three years. As a result, items on the scale were initially modified and then repeatedly tested across each wave. The researchers also conducted confirmatory factor analyses and presented the factor loadings of the constructs. The items on the privacy self-efficacy scale (Zeissig et al., 2017) were generated based on insights from extensive literature reviews about self-efficacy from PMT as it pertained to an individual's privacy online. Items on the response efficacy and privacy protective behaviors scales developed by Boerman et al. (2018) were based on previous studies that measured protective behaviors. In this study, statistical analyses were used to check for any issues with multicollinearity across all relevant variables of interest to determine any issues with convergent/discriminant validity.

It is also imperative to address the method of data collection and potential biases that it can bring to the data, specifically the use of MTurk to gather responses from individuals. Using MTurk to survey individuals has a lot of benefits, but there is skepticism around the use of technology with respect to potential issues of validity and bias in the responses gained. Rouse (2015) found that issues pertaining to the validity of responses could be mitigated by adding checks for attentiveness of the respondents. In addition to this, simple intelligence-type questions can be built in towards the beginning of the survey to address potential challenges from inattention and other biases. The current study reported all details surrounding data collection (apart from any

information that would be detrimental to the respondents, regardless of the anonymization already in place) so that if the study or parts of it were to be replicated, all demographic information from the sample can be closely emulated in future works involving the use of MTurk or convenience samples.

3.5 Validity and Reliability of SE Susceptibility Scale

The reliability and validity of the scale developed to measure the susceptibility to social engineering attacks were assessed in the following ways. Prior to data collection, all the scenarios were evaluated to determine if they were representative of legitimate communications and social engineering attacks. The scenarios that were used in the survey were partly collected from public sources online, and partly collected from communications received by the author.

A principal component factor analysis, using varimax rotation, was conducted on the 21 items on the susceptibility scale. The Kaiser-Meyer-Olkin measure of sampling adequacy was .87, which was well over the recommended value of .5 (Kaiser & Rice, 1974). Bartlett's test of sphericity was significant ($\chi^2(210) = 1924.74$, $p < .001$). The communalities for all items were above .3, indicating that all items shared common variance with each other. The eigenvalues obtained for all the items in the scale indicated four factors with eigenvalues over Kaiser's criterion of 1. These four factors together explained 54.09% of the variance across all items. The scree plot generated indicated that the point of inflexion would justify retaining three or four factors. Based on the factor loadings, four factors were initially retained for analysis. The first factor included items that measured susceptibility to pharming attacks based on legitimate scenarios. This factor accounted for 14.44% of the total variance. The second factor included items that measured susceptibility to phishing and smishing attacks based on social engineering-type scenarios. This factor accounted for 14.22% of the total variance. The third factor included items that measured susceptibility to phishing and smishing attacks based on legitimate scenarios. This factor accounted for 13.503% of the total variance. Finally, the fourth factor included items that measured susceptibility to pharming attacks based on social engineering-type scenarios. This factor accounted for 11.92% of the total variance. The factor loadings are summarized in Table 3.1. Based on reliability analyses, the overall reliability of the scale was good, Cronbach's $\alpha = .87$.

Table 3.1 Factor loadings and communalities based on principal components analysis for 21 items on Susceptibility to Social Engineering Scale (n = 272)

Scale Item	Factor loading				Communalities
	1	2	3	4	
Email 1			.63		.55
Email 2			.62		.51
Email 3			.38		.36
Message 1			.56		.49
Message 2			.48		.54
Message 3			.42		.50
Smish 1			.65		.49
Smish 2		.52			.49
Smish 3		.74			.59
Smish 4		.40			.50
Phish 1		.67			.61
Phish 2		.48			.45
Phish 3		.39			.35
Phish 4		.67			.51
Website 1	.76				.60
Website 2	.79				.66
Website 3	.81				.69
Pharm 1				.65	.54
Pharm 2				.68	.61
Pharm 3				.78	.67
Pharm 4				.73	.65

Note. n = 272. The extraction method was principal components with a varimax rotation. The highest factor loadings, above .3, are represented.

As the scale covered susceptibility to three types of social engineering attacks, the scale was broken down into three subscales to determine factor loadings and the reliabilities of the subscales. These subscales were the phishing, smishing and pharming susceptibility subscales respectively. A principle component factor analysis, using varimax rotation, was conducted on the 7 items of all three subscales respectively. For each subscale, the items loaded on two factors. All legitimate scenarios loaded on one factor, and all social engineering scenarios loaded on the other factor. Overall, the factor loadings indicated that all constructs were represented accurately. The summary of the factor loadings for the smishing subscale can be found in Table 3.2, the factor loadings for the phishing subscale can be found in Table 3.3, and the factor loadings for the

pharming subscale can be found in Table 3.4. Subsequent reliability analyses also indicated good reliabilities for the phishing (α = .73), smishing (α = .77) and pharming (α = .75) subscales.

Table 3.2 Factor loadings and communalities based on principal components analysis for 7 items on Susceptibility to Smishing Subscale (n = 272)

Scale Item	Factor loading		Communalities
	1	2	
Message 1		.63	.55
Message 2		.62	.56
Message 3		.88	.79
Smishing 1	.48		.46
Smishing 2	.68		.56
Smishing 3	.73		.54
Smishing 4	.75		.56

Note. n = 272. The extraction method was principal components with a varimax rotation. Factor loadings above .3 are represented.

Table 3.3 Factor loadings and communalities based on principal components analysis for 7 items on Susceptibility to Phishing Subscale (n = 272)

Scale Item	Factor loading		Communalities
	1	2	
Email 1	.72		.53
Email 2	.79		.63
Email 3	.65		.45
Phishing 1		.76	.61
Phishing 2		.63	.46
Phishing 3		.49	.49
Phishing 4		.78	.61

Note. n = 272. The extraction method was principal components with a varimax rotation. Factor loadings above .3 are represented.

Table 3.4 Factor loadings and communalities based on principal components analysis for 7 items on Susceptibility to Pharming Subscale (n = 272)

Scale Item	Factor loading		Communalities
	1	2	
Website 1		.79	.63
Website 2		.86	.74
Website 3		.86	.75
Pharming 1	.77		.59
Pharming 2	.70		.56
Pharming 3	.82		.68
Pharming 4	.73		.62

Note. n = 272. The extraction method was principal components with a varimax rotation. Factor loadings above .3 are represented.

CHAPTER 4. DATA ANALYSIS AND RESULTS

This chapter provides an overview of the data screening procedures, the analytical strategies that were employed for hypotheses testing, the descriptive statistics of the sample, and the results of data analysis. A summary of all the results are also provided at the end of the chapter.

4.1 Data Screening

The sample was composed of respondents recruited from MTurk. A total of 301 responses were initially collected. Before data screening, 5 responses were deleted from the dataset as they were merely empty responses generated as a part of the Qualtrics preview function. As these were not actual responses, the empty data points could be deleted from the dataset. An additional 19 responses were deleted from the dataset due to incorrect responses on the attention check questions. As a result, a total of 24 responses were deleted from the survey, leaving 277 responses for data screening and subsequent analysis. The data-screening steps were based on the main assumptions for data used in statistical tests for general linear models, particularly for the social sciences (Field, 2018). Based on those recommendations, an additional two responses were deleted due to missing values from the response efficacy scale, and three responses were deleted as they were identified as multivariate outliers. This left 272 responses from participants for the final analysis.

4.2 Descriptive Statistics

The final sample comprised 272 valid responses from the survey respondents. The majority of respondents were male (n = 171, 62.9%), followed by women (n = 100, 36.8%) and individuals who preferred to not share their gender (n = 1, .40%). The sample also largely constituted respondents between the ages of 25 to 34 years (n = 149, 54.8%). The majority of the sample also identified as white (n = 210, 77.8%). Respondents were also asked to report their education level, and the majority of the sample reported having a bachelor's degree (n = 159, 58.7%). A detailed breakdown of the sample based on these demographics can be found in Table 4.1, with the demographics categorized based on social engineering victimization.

Table 4.1 Demographics for self-reported SE non-victims versus victims

Variable	Non-Victims (n = 68)	Victims (n = 203)	Total (N = 271)
Sex			
Male	45 (66.2)	125 (61.6)	170 (62.7)
Female	22 (32.4)	78 (38.4)	100 (36.9)
Prefer not to say	1 (1.5)	0 (0.0)	1 (0.4)
Age (yrs)			
18-24	2 (2.9)	5 (2.5)	7 (2.6)
25-34	36 (52.9)	112 (55.2)	148 (54.6)
35-44	18 (26.5)	51 (25.1)	69 (25.5)
45-54	6 (8.8)	20 (9.9)	26 (9.6)
55-64	5 (7.4)	13 (6.4)	18 (6.6)
65-74	1 (1.5)	2 (1.0)	3 (1.1)
Ethnicity			
White	58 (85.3)	151 (75.1)	209 (77.7)
Black/African American	3 (4.4)	42 (20.9)	45 (16.7)
Asian	5 (7.4)	7 (3.5)	12 (4.5)
Hispanic/Latino	0 (0.0)	1 (0.4)	1 (0.3)
Prefer not to say	1 (1.5)	0 (0.0)	1 (0.4)
Other	2 (1.4)	1 (1.5)	3 (1.1)
Education Level			
High school graduate	14 (20.6)	8 (4.0)	22 (8.1)
Associate degree	2 (2.9)	13 (6.4)	15 (5.6)
Bachelors' degree	38 (55.9)	121 (59.9)	159 (58.9)
Masters' degree	12 (17.6)	59 (29.2)	71 (26.3)
Doctorate	1 (1.5)	1 (0.5)	2 (0.7)
Prefer not to say	1 (1.5)	0 (0.0)	1 (0.4)

Note. Values represent frequencies with percentages in parentheses. Valid N = 271

Descriptive analyses on social engineering victimization showed that a majority of respondents had been a victim of at least one social engineering attack (n = 203, 74.9%), compared to non-victims (n = 68, 25.1%). Out of all the respondents, 54% reported falling victim to phishing attacks (n = 147), 37.5% reported falling victim to smishing attacks (n = 102), and 30.1% reported falling victim to pharming attacks (n = 82). The majority of respondents also indicated that they had suffered serious consequences as a result of a social engineering attack (n = 168, 61.8%).

According to frequency analyses on the sample, respondents on average scored relatively lower on the measure of actual susceptibility to social engineering attacks (M = 2.60, SD = .64)

compared to their perceived susceptibility to social engineering attacks (M = 3.15, SD = 1.14). When considering susceptibility to the three types of social engineering attacks, respondents on average scored the highest on susceptibility to pharming attacks (M = 2.72, SD = .81), followed by susceptibility to phishing attacks (M = 2.56, SD = .73) and susceptibility to smishing attacks (M = 2.52, SD = .77).

Respondents on average scored higher on the measure of need for privacy (M = 3.68, SD = .70), followed by measure of privacy self-efficacy (M = 3.55, SD = .70), and the measure of response efficacy (M = 2.76, SD = .93). Respondents also on average scored relatively high on the measure of privacy protective behaviors (M = 3.22, SD = .74), in relation to need for privacy and privacy-self efficacy. The results of all frequency analyses are summarized in Table 4.2.

Table 4.2 Summary of frequency analyses on study variables

Variable	*M*	*SD*
Perceived Sus. to SE Attacks	3.15	1.14
Actual Sus. to SE Attacks	2.60	.64
Sus. to Phishing Attacks	2.56	.73
Sus. to Smishing Attacks	2.52	.77
Sus. to Pharming Attacks	2.72	.81
PSE	3.55	.70
PRE	2.76	.93
NFP	3.68	.70
PPB	3.22	.74

Note. N = 272. All variables were measured on a scale from 1-5. *Sus.* = Susceptibility; *PSE* = Privacy Self-Efficacy; *PRE* = Privacy Response-Efficacy; *NFP* = Need for Privacy; *PPB* = Privacy Protective Behaviors

4.3 Analytical Strategies

Initially, a zero-order correlation analysis was run between social engineering victimization and the average scores of susceptibilities to the three types of social engineering attacks investigated in this study. Based on the results, a *t*-test was conducted to support the results of the correlation analysis. Next, zero-order correlations were conducted between the demographic variables and two variables of interest – privacy protective behaviors and susceptibility to social engineering attacks. This was conducted to check if any of the demographic variables needed to be controlled for in subsequent analyses. After this, zero-order correlation analyses were run between all variables of interest from all hypotheses to determine the relationships between all variables. A simple linear regression was conducted to test hypothesis one. Based on the results, a multivariate analysis of variance (MANOVA) was also conducted to determine any average group differences between the average susceptibility scores of the three types of social engineering attacks, based on low and high levels of engagement in privacy protective behaviors. A multiple linear regression was then conducted to test hypotheses two through five.

4.4 Analysis Results

A two-tailed, zero-order correlation analysis was run between social engineering victimization and susceptibility scores for the three types of social engineering attacks (susceptibility to phishing, smishing and pharming attacks respectively) to determine any significant relationships between victimization and the extent to which an individual might be susceptible to the specific types of attacks studied in this study. The correlation analysis indicated that only susceptibility to pharming attacks was statistically significantly related to social engineering victimization, r_{pb} = -.14, p = .02. This suggested a negative relationship between susceptibility to pharming and general victimization, implying that individuals who have been victims of social engineering attacks are less likely to be susceptible to pharming attacks. The results of this correlation analysis are summarized in Table 4.3.

Table 4.3 Zero-order correlations between victimization and average susceptibilities scores

	SE Victim.	Phishing Score	Smishing Score	Pharming Score
SE Victim.	1	-.02	.04	-.14*
Phishing Score		1	.68**	.56**
Smishing Score			1	.39**
Pharming Score				1

** $p < .01$, * $p < .05$, two-tailed

Listwise $N = 271$

Note. SE Victim. = Social Engineering Victimization; *Phishing Score* = Average score on susceptibility to phishing attacks; *Smishing Score* = Average score on susceptibility to smishing attacks; *Pharming Score* = Average score on susceptibility to pharming attacks

An independent samples *t*-test was run to determine the group differences between victims and non-victims of social engineering attacks on susceptibility to pharming attacks. The results of this analysis indicated that on average, non-victims were more susceptible to pharming attacks ($M = 2.92$, $SE = .09$) than victims ($M = 2.66$, $SE = .06$). This test was found to be statistically significant, $t(269) = 2.37$, $p = .02$, and represented a small effect size, $r_{pb} = .14$. The results of this analysis are also summarized in Table 4.4.

Table 4.4 Results of independent samples *t*-test

Variable	Non-Victim ($n = 68$)		Victim ($n = 203$)		*t*	*p*
	M	*SD*	*M*	*SD*		
Average score on Pharming Susceptibility	2.92	.71	2.66	.84	2.37	.02

Note. The results of the test were based on assumption of equal variances ($p = .12$)

A two-tailed, zero-order correlation analysis was run between privacy protective behaviors and susceptibility to social engineering attacks, and the demographic variables, to account for any demographic variables that would need to be controlled for. The correlation analysis indicated that none of the demographic variables had significant relationships with privacy protective behaviors and susceptibility to social engineering attacks respectively, as shown in Table 4.5.

Table 4.5 Zero-order correlations between demographics, privacy protective behaviors, and susceptibility to SE attacks

	PPB	SE Sus.	Age	Gender	Ethnicity	Education Level
PPB	1	-.31**	-.11	-.01	-.02	.08
SE Sus.		1	.09	.06	.11	-.11
Age			1	.01	.09	.00
Gender				1	.01	.10
Ethnicity					1	.16**
Education Level						1

* $p < .01$, two-tailed

Listwise $N = 269$
Note. PPB = Privacy Protective Behaviors; *SE Sus.* = Susceptibility to Social Engineering Attacks

A one-tailed, zero-order correlation analysis was also conducted between all the main variables of interest – privacy protective behaviors, susceptibility to social engineering attacks, social engineering victimization, need for privacy, privacy self-efficacy, and privacy response efficacy, as shown in Table 4.3. The correlation analysis indicated that there was a statistically significant relationship between privacy protective behaviors and susceptibility to social engineering attacks ($r = -.31$, $p < .01$), suggesting that individuals who engage in privacy protective behaviors are less likely to be susceptible to social engineering attacks.

There was a statistically significant relationship between privacy protective behaviors and social engineering victimization ($r_{pb} = .15$, $p < .01$), suggesting that individuals who reported being victims of social engineering attacks engaged in more privacy protective behaviors. There were also statistically significant relationships between privacy protective behaviors and privacy self-efficacy ($r = .14$, $p < .05$) and privacy response efficacy respectively ($r = -.17$, $p < .01$), suggesting that individuals who scored high on privacy self-efficacy and low on response efficacy respectively engaged in more privacy protective behaviors. The results of all zero-order correlations are summarized in Table 4.6.

Table 4.6 Zero-order correlations between study variables

	PPB	SE Sus.	SE Victim.	NFP	PSE	PRE
PPB	1	-.31**	.15**	.10	.14*	-.17**
SE Sus.		1	-.05	-.34**	-.38**	.41**
SE Victim.			1	.06	.16**	-.12*
NFP				1	.57**	-.62**
PSE					1	-.60**
PRE						1

** $p < .01$, * $p < .05$, one-tailed
Listwise $N = 271$
Note. PPB = Privacy Protective Behaviors; *SE Sus.* = Susceptibility to Social Engineering Attacks; *SE Victim* = Social Engineering Victimization; *NFP* = Need for Privacy; *PSE* = Privacy Self-Efficacy; *PRE* = Privacy Response Efficacy

Hypothesis 1: Individuals who engage in privacy protective behaviors are less likely to be susceptible to social engineering attacks

The zero-order correlation analysis indicated that there was a statistically significant relationship between engagement in privacy protective behaviors and susceptibility to social engineering attacks, $r = -.31$, $p < .01$. This suggested that susceptibility to social engineering attacks was negatively correlated with engagement in privacy protective behaviors, suggesting that individuals who engaged in privacy protective behaviors were less susceptible to social engineering attacks. This supported hypothesis 1.

A forced entry linear regression was run to determine if engagement in privacy protective behaviors could predict an individual's susceptibility to social engineering attacks. The regression model generated accounted for 9.5% of the variance observed in the outcome variables ($R^2 = .10$), implying that engagement in privacy protective behaviors could explain 9.5% of the variance in an individual's susceptibility to social engineering attacks. This model was found to be statistically significant for understanding the relationship between the predictor and outcome variables, according to the ANOVA analysis ($F(1, 270) = 28.24$, $p < .001$). Therefore, engagement in privacy protective behaviors was found to be a statistically significant predictor of susceptibility to social engineering attacks ($t = -5.31$, $p < .001$). The results overall supported hypothesis 1.

To further understand the relationship between privacy protective behaviors and susceptibility to social engineering attacks, a one-way multivariate analysis of variance (MANOVA) was conducted. This was done to investigate the group differences in average scores of the three types of susceptibility based on low and high levels of engagement in privacy protective behaviors. This statistical technique was chosen over multiple *t*-tests to account for the correlations between all three outcome variables (Field, 2018). Privacy protective behaviors was recoded into a dichotomous variable for analysis, with scores falling under the mean ($M = 3.21$) constituting low levels of engagement, and scores above the mean as high levels of engagement. The analysis indicated a statistically significant difference across the average scores of susceptibilities to the three types of social engineering attacks based on low and high levels of engagement in privacy protective behaviors, $F(3, 268) = 4.11$, $p < .01$, Wilk's $\lambda = .96$, partial $\eta^2 = .04$. A follow-up analysis indicated that there were significant group differences between average scores of phishing susceptibility, ($F(1, 270) = 11.39$, $p < .01$, partial $\eta^2 = .04$), average scores of smishing susceptibility. ($F(1, 270) = 4.15$, $p = .04$, partial $\eta^2 = .02$), and the average scores of pharming susceptibility ($F(1, 270) = 7.14$, $p = .01$, partial $\eta^2 = .03$), demonstrating that low levels of engagement had significantly higher means on susceptibility scores than high levels of engagement. The comparison of effect sizes indicated that susceptibility to phishing was most impacted by engagement in privacy protective behaviors, followed by susceptibility to pharming and susceptibility to smishing attacks respectively. The results of this analysis are summarized in Table 4.7.

Table 4.7 Summary of results of one-way MANOVA

Variable	*df*	MS	*F*	*p*
Phishing Score	1	5.78	11.39	.001
Smishing Score	1	2.43	4.15	.043
Pharming Score	1	4.61	7.14	.008

Note. *Phishing Score* = Average score on susceptibility to phishing attacks; *Smishing Score* = Average score on susceptibility to smishing attacks; *Pharming Score* = Average score on susceptibility to pharming attacks

A forced entry multiple linear regression was run to determine if an individual's social engineering victimization, and their scores on need for privacy, privacy self-efficacy and privacy response efficacy would emerge as predictors of engagement in privacy protective behaviors in the regression model. The model generated by SPSS accounted for 4.7% of the variance observed in the outcome variable (R^2 = .05). This model was found to be statistically significant for understanding the relationship between the predictor variables and the outcome variable, according to the ANOVA analysis (F (4, 266) = 3.30, p = .01). Among all the predictor variables in the model, social engineering victimization (t = 2.13, p = .03) and privacy response efficacy (t = -1.65, p = .01) were significant predictors of engagement in privacy protective behaviors. The collinearity statistics, namely the tolerance and VIF values, did not indicate any issues with multicollinearity across all models (Tolerance > .2 and VIF < 10). The collinearity diagnostics table also indicated no issues with multicollinearity; all condition index values were below 30 and no row in variance proportions had more than one value over .50. Therefore, the regression model had no issues with multicollinearity. The results of this analysis are summarized in Table 4.8.

Table 4.8 Multiple regression predicting engagement in privacy protective behaviors

Variable	*B*	*SE B*	*β*
NFP	-0.03	0.09	-0.03
PSE	0.06	0.08	0.06
PRE	-0.11	0.07	-0.14*
SE Victim.	0.22	0.10	0.13*

* $p < .05$

Note. NFP = Need for Privacy; *PSE* = Privacy Self-Efficacy; *PRE* = Privacy Response Efficacy; *SE Victim*. = Social Engineering Victimization

Hypothesis 2: Individuals who score high on privacy self-efficacy are more likely to engage in privacy protective behaviors

The zero-order correlation analysis indicated that there was a statistically significant relationship between privacy-self efficacy and engagement in privacy protective behaviors, r = .14, $p < .05$. This suggested that privacy self-efficacy was positively correlated with engagement in privacy protective behaviors, meaning that individuals who express higher privacy self-efficacy score higher on engagement in privacy protective behaviors.

The results of the multiple regression analysis indicated that privacy self-efficacy did not significantly predict engagement in privacy protective behaviors ($t = .70$, $p = .48$). While the results of the correlation signified a significant relationship, the results of the multiple regression ultimately reject the hypothesis.

Hypothesis 3: Individuals who score high on privacy response efficacy are more likely to engage in privacy protective behaviors

The zero-order correlation analysis indicated that there was a statistically significant relationship between response self-efficacy and engagement in privacy protective behaviors, $r = -.17$, $p < .01$. This suggested that privacy response efficacy was negatively correlated with engagement in privacy protective behaviors, meaning that individuals who express higher privacy response efficacy score lower on engagement in privacy protective behaviors. While this is a statistically significant finding, it does not directionally support hypothesis 3.

The results of the multiple regression analysis indicated that privacy response efficacy significantly predicted engagement in privacy protective behaviors ($t = -1.65$, $p = .01$). This implied that an individual's engagement in privacy protective behaviors can be predicted based on how they perceive the efficacy of privacy responses.

Hypothesis 4: Individuals who have been victims of social engineering attacks are more likely to engage in privacy protective behaviors

The zero-order correlation analysis indicated that there was a statistically significant relationship between social engineering victimization and engagement in privacy protective behaviors, $r_{pb} = .15$, $p < .01$. This suggested that social engineering victimization was positively correlated with engagement in privacy protective behaviors, meaning that individuals who reported being victims of social engineering attacks were more likely to engage in privacy protective behaviors.

The results of the multiple regression analysis indicated that social engineering victimization significantly predicted engagement in privacy protective behaviors ($t = 2.13$, $p = .03$). This implied that an individual's engagement in privacy protective behaviors can be predicted

based on whether they have been a victim of social engineering attacks in the past. The results of the correlation and regression analyses support hypothesis 4.

Hypothesis 5: Individuals who score high on the need for privacy are more likely to engage in privacy protective behaviors

The zero-order correlation analysis indicated that there was no statistically significant relationship between the need for privacy and engagement in privacy protective behaviors, $r = .10$, $p = .06$.

The results of the multiple regression analysis also indicated that the need for privacy did not significantly predict engagement in privacy protective behaviors ($t = -.36$, $p = .72$). Overall, the results of the correlation and regression analyses reject hypothesis 5.

Of the variables acting as statistically significant antecedents to privacy protective behaviors, privacy response efficacy was also significantly correlated with susceptibility to social engineering attacks ($r = .41, p < .01$), implying that individuals who score high on privacy response efficacy are more likely to be susceptible to social engineering attacks. To explore this further, a mediation analysis was conducted between the three variables to determine if engagement in privacy protective behaviors acted as a mediator between privacy response efficacy and susceptibility to social engineering attacks. To conduct this analysis, the PROCESS tool developed by Hayes (2017) was used to model the relationship. PROCESS is a modeling tool that can be used to estimate direct and indirect effects of mediators on a relationship between an independent and dependent variable (Hayes, 2017). As the variables in the mediation analysis follow the same set of assumptions for regression analyses (Abu-Bader & Jones, 2021), the assumptions of normality, linearity and homoscedasticity were met. To examine the conditions for mediation, linear regressions were run between the dependent (susceptibility to social engineering attacks), independent (privacy response efficacy) and mediator (privacy protective behaviors) variables respectively. As determined from the hypotheses, privacy response efficacy significantly predicted engagement in privacy protective behaviors, and privacy protective behaviors significantly predicted susceptibility to social engineering attacks.

A linear regression was then conducted between privacy response efficacy and susceptibility to social engineering attacks to check the third condition. According to the results of the third regression analysis, the regression model generated accounted for 17.1% of the variance observed in the outcome variable (R^2 = .17), implying that privacy response efficacy could explain 17.1% of the variance in an individual's susceptibility to social engineering attacks. This model was found to be statistically significant for understanding the relationship between the predictor and outcome variable, according to the ANOVA analysis (F (1, 270) = 55.69, p < .001). Therefore, privacy response efficacy was found to be a statistically significant predictor of susceptibility to social engineering attacks (t = 7.46, p < .001), thereby meeting the third condition for mediation analysis.

The mediation analysis was then conducted using SPSS Process Macro to determine if privacy protective behaviors significantly mediated the relationship between privacy response efficacy and susceptibility to social engineering attacks. The results of the regression analysis indicated that privacy response efficacy was a significant predictor of privacy protective behaviors, the mediator (t = -1.65, p = .01). In the next analysis, the mediator was controlled for, and the results of the second regression analysis indicated that privacy response efficacy was a significant predictor of susceptibility to social engineering attacks (t = 6.88, p < .001). The results of the indirect effect of predictor on the outcome variable, based on 5000 bootstrapped samples, showed an indirect positive relationship mediated by privacy protective behaviors, b = .03, 95% CI [.003, .063]. Privacy protective behaviors accounted for 9.7% of the total effect on susceptibility to social engineering attacks. The results of the mediation analysis are graphically represented in Figure 4.1 and summarized in Table 4.9.

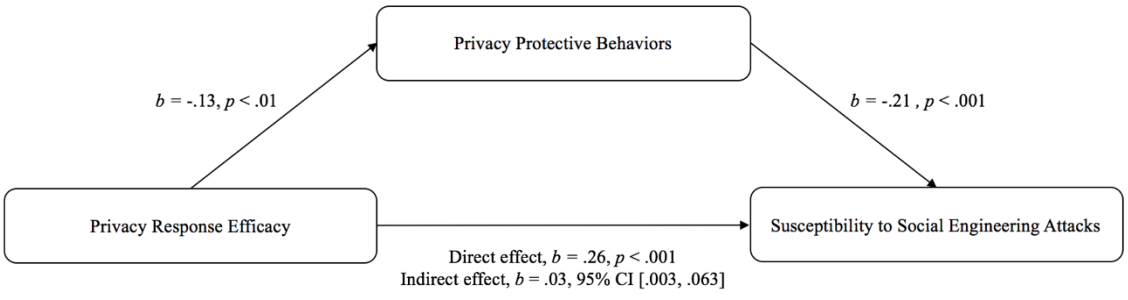


Figure 4.1 Model of Mediation Analysis

Table 4.9 Summary of mediation analysis

Variable/Effect	*b*	*SE*	*t*	*95% Confidence Interval*	
				LL	*UL*
PRE → SE Sus.	0.26	0.04	6.88**	0.18	0.33
PRE → PPB	-0.13	0.05	-2.74*	-0.23	-0.04
PRE → PPB → SE Sus.	-0.21	0.05	-4.53**	-0.31	-0.12
Effects					
Direct	0.26	0.04	6.88**	0.18	0.33
Indirect	0.03	0.02		0.003	0.063
Total	0.29	0.04	7.46**	0.21	0.36

** $p < .001$, * $p < .01$
Based on 5000 bootstrap samples
Note. PRE = Privacy Self Efficacy, *SE Sus.* = Susceptibility to Social Engineering Attacks, *PPB* = Privacy Protective Behaviors
LL = Lower Limit; *UL* = Upper Limit. If interval does not contain zero, it indicates a significant effect

4.5 Summary of Results

Overall, the results of the data analysis suggested that there were some significant relationships between some of the variables of interest from the hypotheses. There was a statistically significant relationship between engagement in privacy protective behaviors and susceptibility to social engineering attacks, suggesting that individuals who engaged in higher levels of privacy protective were less susceptible to social engineering attacks. Looking at the relationships between specific antecedents of privacy and engagement in privacy protective behaviors, privacy self-efficacy, privacy response-efficacy and social engineering victimization were all significantly correlated with engagement in privacy protective behaviors. Contrary to what was hypothesized, the psychological need for privacy was not significantly related to engagement in privacy protective behaviors. Of the significantly related antecedents, privacy response efficacy and social engineering victimization emerged as significant predictors of engagement in privacy protective behaviors. This suggests that individuals who have been victims of social engineering attacks, and perceive existing privacy measures and responses to be inadequate in protecting their privacy online, are more likely to engage in privacy protective behaviors. The results of the subsequent mediation analysis also suggested that privacy protective behaviors acted as a

significant mediator between privacy response-efficacy and susceptibility to social engineering attacks. This would imply that based on perceptions towards social engineering attacks and existing privacy responses, individuals might engage in privacy protective behaviors as a means of reducing their susceptibility to social engineering attacks.

CHAPTER 5. DISCUSSION

This chapter provides a discussion of the results within the context of relevant literature and findings about social engineering and privacy.

The aim of this thesis was to understand the relationship between online privacy and social engineering. Specifically, this thesis aimed to determine if engagement in privacy protective behaviors could influence the extent to which an individual was susceptible to social engineering attacks. It also aimed to understand if specific antecedents of privacy protective behaviors, drawn from the context of protection or self-preservation from social engineering attacks, influenced engagement in privacy protective behaviors and therefore SE susceptibility. The hypotheses tested in this study were developed based on findings from extant literature related to social engineering and privacy, and the intersection of these two fields. The concept of the psychological need for privacy, and the theory of protective motivation were both used to guide the development of the research design. The sample for data collection comprised users of Amazon MTurk who were residents of the United States. The final dataset contained 272 responses for data analysis. Overall, the hypotheses assessed the relationships of four specific antecedents of privacy protective behaviors, and the relationship between privacy protective behaviors and susceptibility to social engineering attacks. The results from the final data analysis indicated that some of the hypotheses were fully or partially supported, while others were rejected.

5.1 Discussion of Demographics

Initial correlation analyses indicated that the demographic variables of age, gender, ethnicity and education level did not have significant correlations with susceptibility to social engineering attacks. The effects of age and gender on social engineering susceptibility have been studied in literature, with individuals older in age being more susceptible to social engineering attacks (Darwish et al., 2012; Sheng et al., 2012), and females being more susceptible to social engineering attacks (Darwish et al., 2012; Halevi et al., 2013; Hong et al., 2013; Uebelacker & Quiel, 2014). However, more recent findings have indicated no significant effects of gender on susceptibility (Abbasi et al., 2016; Bullée et al., 2017; Montañez et al., 2020), thereby supporting the findings

from this study. Similarly, findings on the impact of age on susceptibility or on correct identification of social engineering attacks indicate mixed results, with some studies suggesting positive (Lin et al., 2019), negative (Sheng et al., 2012) or no effects (Bullée et al., 2017) of age on susceptibility to social engineering attacks. These non-significant effects could potentially be attributed to the extent to which individuals interact with technology, and by extension the extent to which the average person is on the receiving end of social engineering attacks. The results of this study indicated that on average, individuals were actually less susceptible to social engineering attacks than they perceived themselves to be. While studies about awareness and susceptibility have indicated that individuals are largely unaware of the different persuasive tactics that can be used across social engineering attacks (Aldawood & Skinner, 2019; Bakhshi, 2017), there is also evidence to suggest that individuals can better identify attack instances after undergoing some form of awareness/education training (Smith et al., 2013).

Similarly, findings from literature about the relationships between demographics and online privacy are also mixed, with results suggesting no effects between most demographic variables and online privacy concerns and behaviors (Boerman et al., 2018; Hazari & Brown, 2013; Yao et al., 2007). This largely lent support to the findings of this study. As the scope of this study was restricted to individuals in the United States alone, the non-significant findings provide some more perspective to our understanding of how perceptions of privacy might differ based on locations, specifically across parts of the world that have stringent regulations on the preservation of consumer privacy.

5.2 Discussion of Hypothesis 1

Hypothesis 1 stated that individuals who engaged in privacy protective behaviors were less likely to be susceptible to social engineering attacks. The results of the analysis supported this hypothesis, with engagement in privacy protective behaviors acting as a significant predictor of lowered susceptibility to social engineering attacks. Further analyses also supported the notion that high levels of engagement in privacy protective behaviors could also help reduce susceptibility to the specific types of social engineering attacks investigated in this study – phishing, smishing and pharming attacks respectively. This finding holds major implications for how we approach defenses against social engineering attacks. For the most part, countermeasures emphasize changes in how people address communications that can be social engineering attacks, from identifying the

persuasive techniques used in communications to elicit information (Schaab et al., 2017), to robust and comprehensive employee education that addressed virtual and physical modes of human-based social engineering attacks (Peltier, 2006). The significance of this finding is the use of existing behaviors as a means of addressing the threats posed from social engineering attacks. The major implication of this finding is that if people engage in privacy protective behaviors, even if it were for the intent of controlling personal information alone, they would still be able to protect themselves from social engineering attacks.

5.3 Discussion of Hypothesis 2

Hypothesis 2 stated that individuals who scored high on privacy self-efficacy were more likely to engage in privacy protective behaviors. The results showed that privacy self-efficacy was significantly positively correlated with engagement in privacy protective behaviors, but was not a significant predictor of engagement in those behaviors. In the scope of this study, privacy self-efficacy was defined as the perceived capability of an individual in maintaining their online privacy (LaRose & Rifon, 2007). This is distinct from, but could also be understood as a subset of, general self-efficacy, which refers to the perceived capability of an individual in performing difficult tasks or coping with specific adversities across different areas of life (Schwarzer & Jerusalem, 1995). The results suggested that individuals who expressed higher capabilities in maintaining their online privacy were likely to engage in privacy protective behaviors, but this capability was not a significant predictor of engagement in the behaviors. The results indicated that hypothesis 1 was not fully supported.

This could be potentially explained by viewing privacy self-efficacy in the context of information disclosure. In their work investigating the influence of privacy self-efficacy on actual management of privacy settings online, Chen and Chen (2015) found that privacy self-efficacy was positively associated with privacy protective actions, but did not reduce information disclosure itself. They speculated that users could feel confident about handling any issues or threats to their online privacy, but restricting the amount of information they shared online would not be considered a method of handling threats to online privacy. Privacy protective behaviors, in the context of information privacy, are considered actions that individuals take to restrict or control access to their information online from other entities. Therefore, individuals can express high levels of privacy self-efficacy, but that does not mean that they would necessarily engage in the

behaviors that can protect their privacy online. Another explanation for this could be found in context-based experiences. In their study on understanding privacy judgements based on how experienced individuals were with using mobile applications, Martin and Shilton (2015) found that individuals who frequently used applications made privacy judgements based on the context of the application itself, as opposed to the general beliefs they held about maintaining their privacy. This could be applied to the understanding of self-efficacy with respect to engagement in protective behaviors – individuals might feel fairly confident about their capabilities of protecting their online privacy, but may not feel the need to actually engage in those behaviors due to the context of their online environments.

5.4 Discussion of Hypothesis 3

Hypothesis 3 stated that individuals who scored high on privacy response efficacy were more likely to engage in privacy protective behaviors. The results showed that privacy response efficacy was significantly negatively correlated with engagement in privacy protective behaviors. The regression analysis also showed that privacy response efficacy is a significant predictor of engagement in privacy protective behaviors, implying that individuals who express higher levels of response efficacy exhibit lower engagement in privacy protective behaviors. While the results are statistically significant, they are directionally opposite to what was hypothesized and to the findings from literature that the hypothesis was based on (Boerman et al., 2018). Existing literature on privacy response efficacy as a specific construct is quite limited, but there are studies and reports that have investigated how specific privacy responses (or measures or affordances, depending on how they are defined or operationalized in literature), are related to engagement in privacy protective behaviors. This can provide some insights into the results related to this hypothesis. In this study, privacy response efficacy refers to the extent to which individuals believe that existing protective measures can actually protect their online privacy. The motivation behind this hypothesis was that individuals could be confident in the utility of their actions if they believed that existing tools and measures in place were also useful and effective against threats to privacy. The implications of the results however are that if the effectiveness of these protective measures is gauged as low, individuals would engage in more privacy protective behaviors, so as to extend control over all aspects of their personal information online.

However, it is also likely that the trust that individuals place in these affordances can result in them not engaging in protective behaviors on their part. Part of this can be attributed to the complexities of privacy measures. For example, privacy policies often provide a comprehensive overview of the different terms and conditions associated with privacy settings, but the onerous nature of actually reading through a privacy policy practically ensures that individuals largely do not engage in the action of reading the policy, opting instead to simply click through when prompted (Kerry, 2019). Recent research on Americans' attitudes about and experiences with privacy indicated that a great percentage of individuals surveyed indicated that privacy protective tools that allowed them to control their information online would be effective in maintaining their online privacy and protecting their personal information online, compared to laws or policies from governments and companies respectively (Auxier et al., 2020). This implies that if individuals perceive privacy measures to be effective in affording them control over how their personal information is hosted and shared online, they would be less likely to engage in distinctive protective behaviors, or even privacy protective behaviors that are enabled by the privacy measures. This can be explained by the feelings of confusion surrounding online privacy on a whole, and the lack of confidence in the entities that maintain the privacy of information online. A report on American consumer activity with respect to privacy found that 96% of Americans surveyed believed that companies had to be more responsible for assuring privacy (Moskowitz, 2020), implying that the responsibility of maintaining privacy online would fall more on companies than on individuals themselves. Another factor that could potentially explain the directional difference in the hypothesis is the privacy paradox. The privacy paradox refers to the dichotomy between privacy attitudes and privacy behaviors. In simpler terms, the privacy paradox contends that individuals care a lot about their privacy, but engage in behaviors that are contrarian to assuring privacy (Kokolakis, 2017). As such, it can be argued that individuals might gauge the effectiveness of privacy responses as pertinent to assuring their online privacy, but may not actually engage in the protective behaviors that are enabled by these responses.

5.5 Discussion of Hypothesis 4

Hypothesis 4 stated that individuals who have been victims of social engineering attacks were more likely to engage in privacy protective behaviors. The results showed that there was a significant correlation between victimization and engagement in protective behaviors, with social

engineering victimization also acting as a significant predictor of privacy protective behaviors. This implies that individuals who have been victims of social engineering attacks in the past, regardless of number, would be more likely to engage in privacy protective behaviors. This finding was in line with evidence from literature (Algarni, 2019; Chen et al., 2017; Cho et al., 2009; Montañez et al., 2020), suggesting that individuals learn from their past experiences and are careful about they disclose their information online. Overall, hypothesis 4 was supported through this study.

5.6 Discussion of Hypothesis 5

Hypothesis 5 stated that individuals who scored high on the need for privacy would be more likely to engage in privacy protective behaviors. The results showed that need for privacy was not significantly correlated with engagement in privacy protective behaviors, therefore contradicting the overarching viewpoint held in literature that an individual's inherent need for privacy acts as a motivator of engagement in privacy protective behaviors. Studies that directly studied the relationships between the need for privacy and privacy protective behaviors indicated unanimously that individuals scoring high on the need for privacy were less likely to utilize social media and more likely to restrict the amount of information that they disclosed about themselves online, which would in turn impact the extent of engagement in privacy protective behaviors (Blachnio et al., 2016; Yao et al., 2007). Surprisingly, the results of this study suggested no significant interactions between the two measures, despite individuals scoring relatively high on the need for privacy measure. This can again be potentially attribute to the privacy paradox, wherein individuals might hold strong attitudes about maintaining their need for privacy, but ignore it in favor of information disclosure for a variety of benefits. Privacy is also a highly dynamic, individually subjective, and contextual construct. Inherent privacy needs can be held constant, but the manifestation of these needs invariably differ across different contexts (Ackerman & Mainwaring, 2005). The measure of need for privacy used in this study measured the general need for privacy, and incorporated items related to the need for information privacy. It is likely that the need for privacy across individuals manifests differently based on the different online environments, but it is also just as likely that the general, psychological need for privacy might not fully translate into engagement of privacy protective behaviors specific to online environments. The scope of this study considered the psychological need for privacy as defined in the

Encyclopedia of Individual and Personality Differences, which considered need for privacy as a need to selectively control access on a general scale, as opposed to online environments alone (Trepte & Masur, 2020). Therefore, while hypothesis 5 was not supported in this study, it also provides the insight that general dispositions towards the need for privacy are arguably not sufficient to encourage engagement in privacy protective behaviors online.

5.7 Discussion of Mediation Model

Overall, two of the five hypotheses were fully supported, one hypothesis was significant but was not directionally supported, and two of the hypotheses were not supported. Results from the regression analysis indicated that privacy response efficacy and social engineering victimization were significant predictors of privacy protective behaviors. This implied that individuals who have been victims of social engineering attacks, and perceive privacy responses as being lowly effective, engage in privacy protective behaviors. Of these, privacy response efficacy also had a significant relationship with susceptibility to social engineering attacks, which suggested that individuals who scored high on privacy response efficacy were more susceptible to social engineering attacks. Therefore, a mediation analysis was conducted between privacy response efficacy, privacy protective behaviors, and susceptibility to social engineering attacks. The results of the mediation analysis indicated a small significant mediation effect of privacy protective behaviors on the relationship between privacy response efficacy and susceptibility to social engineering attacks. What this implies is that engagement in privacy protective behaviors indirectly impacts the relationship between privacy response efficacy and susceptibility to social engineering attacks. This finding provides a relatively unique understanding of how privacy affordances and behaviors interact in order to influence the susceptibility to social engineering attacks. If people do not believe that the existing privacy measures in place are adequate enough to protect their information online, they would engage in more privacy protective behaviors in order to preserve their online privacy. However, this in turn impacts their susceptibility to social engineering attacks, with their susceptibility decreasing due to increased engagement in protective behaviors.

CHAPTER 6. CONCLUSION AND FUTURE WORK

This chapter provides an overview of the limitations associated with this study, the conclusions of the thesis and directions for future research.

6.1 Limitations

One of the limitations of this study is the restriction imposed on the population identified for research. The study population and sample were restricted to the United States. The literature review suggested no significant differences among different groups on privacy protective behaviors and susceptibility to social engineering attacks, but some studies did indicate differences in how online privacy is perceived across different countries (Cullen, 2009; Orito et al., 2008). Therefore, the perceptions of both online privacy and social engineering can differ across different parts of the world based on existing provisions to protect online privacy, and the manner in which people respond to social engineering attempts. The results of this study can only be representative of sentiments held about online privacy and social engineering in the United States.

Another limitation of this study is the use of a convenience sample from MTurk to recruit respondents for the survey. These respondents may not be truly representative of the American, internet-user population. With that said, recruiting respondents from MTurk still managed to provide a different perspective on understanding privacy protective behaviors and susceptibility to social engineering attacks. Most studies that investigated behaviors and susceptibility recruited respondents from universities, thereby providing insights about the relationships only specific to a certain age group. Therefore, the advantage of using MTurk, though a limitation in terms of sampling, was that the respondent pool was fairly diverse and allowed for individuals from a variety of ages to respond to the survey.

Another limitation of this study is the number and types of social engineering attacks that were used for the susceptibility measure. The three most common types of social engineering attacks that were reported in the last year were used for this study, but they do not represent the gamut of human- and technical-based social engineering attacks that individuals experience on a relatively regular basis. Due to scope limitations and the literature surrounding social engineering and privacy, only susceptibility to phishing, smishing, and pharming were assessed in this study.

Depending on the other types of social engineering attacks that could be studied, the impacts of privacy protective behaviors on susceptibility could differ.

This study was also conducted during the novel coronavirus pandemic, during which individuals were exposed to numerous types of scams and messaging surrounding vaccinations and public health measures. Anxieties and fears that individuals have surrounding the pandemic can negatively impact engagement in protective behaviors against social engineering attacks (Abroshan et al., 2021). This could have had impacts on how individuals perceived and classified the scenarios presented in the survey, regardless of the content of the scenarios themselves.

Finally, the susceptibility to social engineering was measured based on scenarios presented to the respondents. While the content of the scale itself mirrors the types of communications that people receive, the scenarios were also delivered through the survey, which is not a faithful representation of the online environments in which individuals receive these communications. It is likely that contextual cues could impact classification of communications as social engineering attempts or legitimate communications. However, as much as possible, the scenarios presented in the survey retained most contextual cues that would be necessary to decide if the scenario was legitimate or a social engineering attempt.

6.2 Conclusions and Future Work

With social engineering attacks continually increasing in current times, it has become increasingly important to address social engineering awareness and protections across individuals so as to protect them from falling victim to these attacks. This study attempted to provide a novel perspective to defenses against social engineering attacks by suggesting existing engagement in privacy protective behaviors as a deterrent to susceptibility to social engineering attacks. Overall, the study provides good support for the encouragement of privacy protective behaviors as a mechanism of defense against social engineering attacks. This study contributes to current understanding about methods of deterrence against social engineering attacks by placing an emphasis on the role of privacy protective behaviors as deterrents. Engagement in privacy protective behaviors not only enables individuals to maintain their privacy, but also can help them stay privy to social engineering attacks. By engaging in protective behaviors, individuals are essentially limiting the extent of access to their information online, which in turn is a major deterrent to social engineering attacks that rely on use of this information to be successful.

Exploring this relationship further could hold the key to refining social engineering awareness and education, and provide some insights into privacy protection as a motivator for individuals to be better educated and prepared against social engineering attacks. However, it is also evident that privacy protection is not the responsibility of the individual alone, but also the entities that provide the platforms for information sharing and the affordances for online privacy protection and control (Yao & Linz, 2008). While engagement in protective behaviors is the responsibility of the individual, there is also evidence to suggest that reliance on existing protective measures from companies and platforms further bolsters privacy protection, and defense against social engineering attacks on a whole. This hold implications for the design and development of privacy affordances on platforms, particularly as it related to information disclosures or even misclosures.

Overall, this study contributes to the body of knowledge about social engineering by providing justification for privacy protective behaviors as a viable means of defending against social engineering attacks. This study also introduced a social engineering susceptibility scale that was comprehensive of the most common types of social engineering attacks that individuals are experiencing in recent times. This contributes to the body of knowledge by introducing susceptibility to smishing and pharming attacks as well, as opposed to just phishing attacks. The results from this study not only supported some of the general findings in literature, but also provided some perspectives on the impacts of specific antecedents of privacy protective behaviors studied in the context of protection from social engineering attacks.

The practical relevance of the study lies in the utility of encouraging individual behaviors in response to increasing social engineering attacks. Regardless of the contextual environment and mode of communication, social engineering attacks like phishing, smishing and vishing still pervade the online space. Almost all individuals who use any mode of information and communication technology experience different forms of social engineering attacks, from scam calls on personal devices to phishing emails on work communications. The difficulty with ascertaining true susceptibility and victimization to social engineering attacks lies in the fact that these attacks are prolific, and that there is no true pattern to who falls victim to social engineering attacks. The findings of this study lend themselves towards practical actions that individuals can take in order to protect themselves from, or at the very least, identify and report social engineering attacks. Defense against social engineering attacks does not have to be reliant on technological countermeasures alone. By emphasizing and bolstering individual capabilities, people can feel

confident in their own abilities to protect themselves from social engineering attacks, without any specific technical knowledge and without complete reliance on technological countermeasures alone. Inculcating or engaging in existing privacy protective behaviors can have major impacts on how people perceive, identify, report, and keep themselves safe from social engineering attack attempts.

The findings from this study lend themselves to different avenues for future works. Future research in the area of social engineering susceptibility could consider how individuals might perceive scenarios when presented with them in the correct contextual environment. In this study, privacy protective behaviors were studied separately from security protective behaviors, but there are some overlaps in behaviors that assure both privacy and security. Detailed research can be carried out on the impact of security protective behaviors on social engineering susceptibility, particularly those behaviors that inadvertently limit attacker interactions with their prospective victims. Another major contribution of this study was studying privacy protective behaviors in relation to privacy self-efficacy and response efficacy, as opposed to general coping appraisals. While the scales used in this study were validated, they still considered self- and response-efficacies within the scope of general online privacy. Future work could also consider the development of more robust scales that consider privacy self-efficacy and response-efficacy specific to different types of online environments, and distinct from the understanding of privacy in offline environments. Finally, compared to other studies conducted about vulnerability or susceptibility to social engineering attacks, this study investigated susceptibility to three different types of social engineering attacks that individuals are likely to encounter in their day to day lives. In reality, there are many different types of attacks that individuals encounter, and not all of them might be familiar enough for individuals to quickly identify it as a social engineering attack. Future works could also investigate susceptibility to other types of social engineering attacks, either by using the approaches detailed in this thesis or through field work.

REFERENCES

Abass, I. A. (2018). Social Engineering Threat and Defense: A Literature Survey. *Journal of Information Security*, *09*(04), 257–264. https://doi.org/10.4236/jis.2018.94018

Abbasi, A., Zahedi, F. M., & Chen, Y. (2016). Phishing susceptibility: The good, the bad, and the ugly. *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*. https://doi.org/10.1109/isi.2016.7745462

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). 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. https://doi.org/10.1109/access.2021.3109091

Abu-Bader, S., & Jones, T. V. (2021). Statistical Mediation Analysis Using the Sobel Test and Hayes SPSS Process Macro. *International Journal of Quantitative and Qualitative Research Methods*, *9*(1), 42–61. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3799204.

Ackerman, M. S., & Mainwaring, S. D. (2005). Privacy issues and human-computer interaction. *Computer*, *27*(5), 19–26.

Aguinis, H., Villamor, I., & Ramani, R. S. (2020). MTurk Research: Review and Recommendations. *Journal of Management*, *47*(4), 823–837. https://doi.org/10.1177/0149206320969787

Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*. Wollongong, NSW; IEEE. 10.1109/TALE.2018.8615162.

Aldawood, H., & Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet*, *11*(3), 73. https://doi.org/10.3390/fi11030073

Algarni, A. (2019). What message characteristics make social engineering successful on Facebook: The role of central route, peripheral route, and perceived risk. *Information*, *10*(6), 211. https://doi.org/10.3390/info10060211

Amazon. (n.d.). Amazon Mechanical Turk. https://www.mturk.com/.

AT&T. (2018, March 23). *Problems with messages tool on my computer.* AT&T Community Forums. Retrieved from https://forums.att.com/conversations/data-messaging-features-internet-tethering/problems-with-messages-tool-on-my-computer/5defd311bad5f2f60609c726?commentId=5defdb01bad5f2f60698a0ad.

Atlassian. (2020, September 21). *Enable subscribers: Statuspage*. Atlassian Support. Retrieved from https://support.atlassian.com/statuspage/docs/enable-subscribers/.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2020, May 26). *Americans' attitudes and experiences with privacy policies and Laws*. Pew Research Center: Internet, Science & Tech. Retrieved from https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/.

Babula, E., Mrzygłód, U., & Poszewiecki, A. (2017). Consumers' Need of Privacy Protection – Experimental Results. *Economics & Sociology, 10*(2), 74–86. https://doi.org/10.14254/2071-789x.2017/10-2/6

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*. arXiv:1901.02672v1

Bakhshi, T. (2017). Social Engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. *2017 13th International Conference on Emerging Technologies (ICET)*. https://doi.org/10.1109/icet.2017.8281653

Bansal, G. (2017). Distinguishing between Privacy and Security Concerns: An Empirical Examination and Scale Validation. *Journal of Computer Information Systems*, *57*(4), 330–343. https://doi.org/10.1080/08874417.2016.1232981

Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*, 55–69. https://doi.org/10.1016/j.tele.2019.03.003

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Bergmann, M. (2008). Testing Privacy Awareness. *The Future of Identity in the Information Society*, *298*, 237–253. https://doi.org/10.1007/978-3-642-03315-5_18

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, *53*, 419–426. https://doi.org/10.1016/j.chb.2015.07.025

Bissell, K., LaSalle, R. M., & Cin, P. D. (2019). (rep.). *Ninth Annual Cost of Cybercrime Study*. Accenture. Retrieved from https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Bit Sentinel. (2020, May 6). *Scams & social engineering during widespread crises*. Bit Sentinel. Retrieved from https://bit-sentinel.com/scams-social-engineering-crises/.

Błachnio, A., Przepiorka, A., Boruch, W., & Bałakier, E. (2016). Self-presentation styles, privacy, and loneliness as predictors of Facebook use in young people. *Personality and Individual Differences*, *94*, 26–31. https://doi.org/10.1016/j.paid.2015.12.051

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, *48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Breda, F., Barbosa, H., & Morais, T. (2017). Social engineering and cyber security. In *Proceedings of the International Conference on Technology, Education and Development*, Valencia, Spain.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology*, *11*(1), 97–115. https://doi.org/10.1007/s11292-014-9222-7

Bullée, J. W. H., Montoya, L., Junger, M., & Hartel, P. H. (2017). Spear phishing in organisations explained. *Information & Computer Security*, *25*(5), 593–613. https://doi.org/10.1108/ics-03-2017-0009

Buss, A. H. (2001). *Psychological dimensions of the self*. Sage Publications.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291–302. https://doi.org/10.1016/j.chb.2017.01.003

Chen, H.-T., & Chen, W. (2015). Couldn't or wouldn't? the influence of privacy concerns and self-efficacy in privacy management on Privacy Protection. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 13–19. https://doi.org/10.1089/cyber.2014.0456

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: global concerns and local responses. *New Media & Society*, *11*(3), 395–416. https://doi.org/10.1177/1461444808101618

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155–159. https://doi.org/10.1037/0033-2909.112.1.155

Cohen, J. (2013). The Concepts of Power Analysis. In *Statistical Power Analysis for the Behavioral Sciences*. Academic Press.

Cox, L. K. (2021, August 25). *26 examples of brilliant email marketing campaigns [template]*. HubSpot Blog. Retrieved from https://blog.hubspot.com/marketing/email-marketing-examples-list.

Crane, C. (2020, October 3). *What is smishing? definition, examples & protection tips*. Security Bloggers Network. Retrieved from https://securityboulevard.com/2020/10/what-is-smishing-definition-examples-protection-tips/.

Crossler, R., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *45*(4), 51–71. https://doi.org/10.1145/2691517.2691521

Cullen, R. (2009). Culture, identity and information privacy in the age of digital government. *Online Information Review*, *33*(3), 405–421. https://doi.org/10.1108/14684520910969871

Darwish, A., El Zarka, A., & Aloul, F. (2012). Towards understanding phishing victims' profile. In *2012 International Conference on Computer Systems and Industrial Informatics.* Sharjah, UAE; IEEE. https://doi.org/10.1109/iccsii.2012.6454454

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Department of Homeland Security. (2020, August 25). *Security Tip (ST04-014)*. Cybersecurity and Infrastructure Security Agency CISA. https://us-cert.cisa.gov/ncas/tips/ST04-014.

Dienlin, T., & Metzger, M. (2019). Who Needs Privacy. https://doi.org/10.31219/osf.io/m23bn

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Electric. (2021). (rep.). *Electric 2021 Cybersecurity Report*. Retrieved from https://www.electric.ai/resources/electric-2021-cybersecurity-report.

Ellis, D. (2021). *7 ways to recognize a phishing email: Email phishing examples*. SecurityMetrics Blog. Retrieved from https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email.

Faja, S., & Trimi, S. (2006). Influence of the web vendor's interventions on privacy-related behaviors in e-commerce. *Communications of the Association for Information Systems*, *17*. https://doi.org/10.17705/1cais.01727

Field, A. P. (2018). *Discovering statistics using IBM SPSS Statistics* (5th ed.). Sage Publications Inc.

Floridi, L. (2005). The Ontological Interpretation of Informational Privacy. *Ethics and Information Technology*, *7*(4), 185–200. https://doi.org/10.1007/s10676-006-0001-7

Fox, P. (2020). *Phishing attacks (article) | cyber attacks*. Khan Academy. Retrieved from https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:cyber-attacks/a/phishing-attacks.

Fox, J. (2021, February 28). *Cybersecurity Statistics for 2021*. https://cobalt.io/blog/cybersecurity-statistics-2021.

Gürses, S. (2014). Can you engineer privacy? *Communications of the ACM*, *57*(8), 20–23. https://doi.org/10.1145/2633029

Halevi, T., Lewis, J., & Memon, N. (2013). Phishing, Personality Traits and Facebook. arXiv:1301.7643v2.

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102–113. https://doi.org/10.1016/j.cose.2017.10.008

Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (2nd ed.). The Guilford Press.

Hazari, S., & Brown, C. (2013). An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. *Journal of Information Privacy and Security*, *9*(4), 31–51. https://doi.org/10.1080/15536548.2013.10845689

Hong, K. W., Kelley, C. M., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2013). Keeping Up With The Joneses: Assessing Phishing Susceptibility in an Email Task. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *57*(1), 1012–1016. https://doi.org/10.1177/1541931213571226

Internet Crime Complaint Center, 2020 Internet Crime Report (2021, March 17). Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

Ivaturi, K., & Janczewski, L. (2011). A Taxonomy for Social Engineering attacks. In *International Conferences on Information Resources Management*. Centre for Information Technology, Organizations and People

Johansen, A. G. (2019, September 12). *What is pharming and how to help protect yourself*. Online Scams. https://us.norton.com/internetsecurity-online-scams-what-is-pharming.html.

Kaiser, H. F., & Rice, J. (1974). Little jiffy, Mark IV. *Educational and Psychological Measurement*, *34*(1), 111–117. https://doi.org/10.1177/001316447403400115

Kerry, C. F. (2019, October 25). *Why protecting privacy is a losing game today-and how to change the game*. Brookings Research. Retrieved from https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

Krämer, N. C., & Schäwel, J. (2020). Mastering the challenge of balancing self-disclosure and privacy in social media. *Current Opinion in Psychology*, *31*, 67–71. https://doi.org/10.1016/j.copsyc.2019.08.003

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Kruikemeier, S., Boerman, S. C., & Bol, N. (2020). Breaching the contract? Using social contract theory to explain individuals' online behavior to safeguard privacy. *Media Psychology*, *23*(2), 269–292. https://doi.org/10.1080/15213269.2019.1598434

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the Privacy Paradox Phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Koyun, A., & Al Janabi, E. (2017). Social Engineering Attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, *4*(6), 7533–7538.

Krebs, B. (2017, December 7). *Phishers are upping their game. so should you.* KrebsonSecurity. Retrieved from https://krebsonsecurity.com/2017/12/phishers-are-upping-their-game-so-should-you/comment-page-1/.

LaRose, R., & Rifon, N. J. (2007). Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. *Journal of Consumer Affairs*, *41*(1), 127–149. https://doi.org/10.1111/j.1745-6606.2006.00071.x

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471–481. https://doi.org/10.1016/j.dss.2012.06.010

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to spear-phishing emails. *ACM Transactions on Computer-Human Interaction*, *26*(5), 1–28. https://doi.org/10.1145/3336141

Lopuch, L. (2021, April 2). *Real-life examples of good and bad cold emails*. Woodpecker Blog. Retrieved from https://woodpecker.co/blog/bad-cold-email-to-good-cold-email-examples/.

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social Engineering: The Neglected Human Factor for Information Security Management. *Information Resources Management Journal (IRMJ)*, *24*(3), 1–8. https://doi.org/10.4018/irmj.2011070101

Ma, Q. (2013). The process and characteristics of phishing attacks - A small international trading company case study. *Journal of Technology Research*, *4*(1).

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Malandrino, D., Scarano, V., & Spinelli, R. (2013). How Increased Awareness Can Impact Attitudes and Behaviors toward Online Privacy Protection. In *2013 International Conference on Social Computing* (pp. 57–62). Virginia; IEEE.

Martin, K., & Shilton, K. (2015). Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications. *Journal of the Association for Information Science and Technology*, *67*(8), 1871–1882. https://doi.org/10.1002/asi.23500

McAfee. (2020, December 7). *New McAfee Report Estimates Global Cybercrime Losses To Exceed $1 Trillion*. McAfee. https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=6859bd8c-9304-4147-bdab-32b35457e629.

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' Protection of Online Privacy and Identity. *Journal of Consumer Affairs*, *38*(2), 217–232. https://doi.org/10.1111/j.1745-6606.2004.tb00865.x

Montañez, R., Golob, E., & Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.01755

Moskowitz, B., Nguyen, S., Cohen, M., & Fahs, G. (2020). *Privacy Front and Center: Meeting the Commercial Opportunity to Support Consumers Rights*. Future of Privacy Forum. Retrieved from https://fpf.org/blog/exploring-consumer-attitudes-about-privacy/.

Mousavizadeh, M., & Kim, D. J. (2015). A Study of the Effect of Privacy Assurance Mechanisms on Self-disclosure in Social Networking Sites from the View of Protection Motivation Theory. In *Thirty Sixth International Conference on Information Systems*. Texas; AISNET.

National Institute of Standards and Technology (NIST). (n.d.). Glossary. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/watering_hole_attack.

National Institute of Standards and Technology (NIST). (n.d.). Glossary. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/INFOSEC#:~:text=NIST%20SP%20800%2D160%20Vol,confidentiality%2C%20integrity%2C%20and%20availability.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48. https://doi.org/10.1162/daed_a_00113

Norman, P., Boer, H., Seydel, E. R., & Mullan, B. (2005). Protection Motivation Theory. In *Predicting and Changing Health Behaviour: Research and Practice with Social Cognition Models* (pp. 70–106). McGraw-Hill Education (UK).

Nyoni, P., & Velempini, M. (2018). Privacy and user awareness on Facebook. *South African Journal of Science*, *114*(5-6), 1–5. https://doi.org/10.17159/sajs.2018/20170103

O'Neil, D. (2001). Analysis of Internet Users' Level of Online Privacy Concerns. *Social Science Computer Review*, *19*(1), 17–31. https://doi.org/10.1177/089443930101900103

Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In *Proceedings of the 5th Conference on Information Technology Education - CITC5 '04*, 177–181. https://doi.org/10.1145/1029533.1029577

Orito, Y., Murata, K., Fukuta, Y., McRobb, S. M. R., & Adams, A. A. (2008). Online Privacy and Culture: Evidence from Japan. In *Proceedings of the Tenth International Conference: Living, Working and Learning Beyond Technology, ETHICOMP 2008*. 614-622. Italy.

Paganini, P. (2020, August 6). *The most common social engineering attacks [updated 2020]*. Infosec Institute. https://resources.infosecinstitute.com/topic/common-social-engineering-attacks/.

Parrish, J. L., Bailer, J. L., & Courtney, J. F. (2009). A Personality Based Model for Determining Susceptibility to Phishing Attacks. *Little Rock: University of Arkansas*, 285–296.

Parthy, P. P., & Rajendran, G. (2019). Identification and prevention of social engineering attacks on an enterprise. In *2019 International Carnahan Conference on Security Technology (ICCST)*. Chennai; IEEE. 10.1109/CCST.2019.8888441.

PassProof. (2020). Retrieved from https://app.passproof.net/.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, *20*(1), 18–28. https://doi.org/10.1108/09685221211219173

Peltier, T. R. (2006). Social Engineering: Concepts and Solutions. *Information Systems Security*, *15*(5), 13–21. https://www.proquest.com/scholarly-journals/social-engineering-concepts-solutions/docview/229581839/se-2?accountid=13360.

Pinterest. (2021). Pinterest Login. Retrieved from https://www.pinterest.com/login/.

Pirim, T., James, T., Boswell, K., Reithel, B., & Barkhi, R. (2008). An Empirical Investigation of an Individual's Perceived Need for Privacy and Security. *International Journal of Information Security and Privacy*, *2*(1), 42–53. https://doi.org/10.4018/jisp.2008010103

Pötzsch, S. (2008). Privacy Awareness: A Means to Solve the Privacy Paradox? *The Future of Identity in the Information Society*, *298*, 226–236. https://doi.org/10.1007/978-3-642-03315-5_17

Price, P. C., Jhangiani, R., & Chiang, I.-C. A. (2015). *Chapter 5: Psychological Measurement*. In Research Methods in Psychology (2nd Canadian Edition). https://opentextbc.ca/researchmethods/chapter/reliability-and-validity-of-measurement/.

Proofpoint. (2021). *What is smishing? examples, protection & more: Proofpoint us*. Proofpoint. Retrieved from https://www.proofpoint.com/us/threat-reference/smishing.

Purdue University. (n.d.). *Qualtrics: Survey Tool*. Qualtrics: Survey Tool | Purdue University. https://www.itap.purdue.edu/services/qualtrics.html.

Purdue University - Information Technology. (n.d.). *SPSS installation instructions*. Shopping - software - instructions - spss - index | Purdue University. https://www.itap.purdue.edu/shopping/software/instructions/spss/index.html.

Rafter, D. (2020, January 10). *Phishing email examples to help you identify phishing scams*. NortonLifeLock. Retrieved from https://us.norton.com/internetsecurity-online-scams-phishing-email-examples.html.

Reddit. (2021). *Login*. reddit.com: Log in. Retrieved from https://www.reddit.com/login/.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rouse, S. V. (2015). A reliability analysis of Mechanical Turk data. *Computers in Human Behavior*, *43*, 304–307. https://doi.org/10.1016/j.chb.2014.11.004

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4), 89. https://doi.org/10.3390/fi11040089

Salgado, J. F. (2002). The Big Five Personality Dimensions and Counterproductive Behaviors. *International Journal of Selection and Assessment*, *10*(1-2), 117–125. https://doi.org/10.1111/1468-2389.00198

Salleh, N., Hussein, R., Mohamed, N., Abdul Karim, N., Ahlan, A. R., & Aditiawarman, U. (2012). Examining Information Disclosure Behavior on Social Network Sites Using Protection Motivation Theory, Trust and Risk. *Journal of Internet Social Networking & Virtual Communities*, *2012*, 1–11. https://doi.org/10.5171/2012.281869

Schaab, P., Beckers, K., & Pape, S. (2017). Social engineering defence mechanisms and counteracting training strategies. *Information & Computer Security*, *25*(2), 206–222. https://doi.org/10.1108/ics-04-2017-0022

Schwarzer, R., & Jerusalem, M. (1995). Generalized self-efficacy scale. *Measures in Health Psychology: A User's Portfolio. Causal and Control Beliefs*, *1*, 35–37.

Sheehan, K. B. (2002). Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, *18*(1), 21–32. https://doi.org/10.1080/01972240252818207

Sheng, S., Holbrook, M. B., Kumaraguru, P., Cranor, L. F., & Downs, J. S. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *CHI '10: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Atlanta; ACM. https://doi.org/10.1145/1753326.1753383.

Sheppard, B. H., Hartwick, J., & Warshaw, P. R. (1988). The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *Journal of Consumer Research*, *15*(3), 325. https://doi.org/10.1086/209170

Siponen, M., Pahnila, S., & Mahmood, A. (2006). Factors Influencing Protection Motivation and IS Security Policy Compliance. In *2006 Innovations in Information Technology*. Dubai; IEEE. 10.1109/INNOVATIONS.2006.301907.

Smith, A., Papadaki, M., & Furnell, S. M. (2013). Improving awareness of social engineering attacks. *Information Assurance and Security Education and Training*, *406*, 249–256. https://doi.org/10.1007/978-3-642-39377-8_29

Sobers, R. (2020, March 29). *64% of Americans Don't Know What to Do After a Data Breach - Do You?* (Survey): Varonis. Inside Out Security Blog. https://www.varonis.com/blog/data-breach-literacy-survey/.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. *International Journal of Information Security and Privacy*, *9*(1), 26–46. https://doi.org/10.4018/ijisp.2015010102

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, *2*, 53–55. https://doi.org/10.5116/ijme.4dfb.8dfd

Tavani, H. T. (2008). Information Privacy: Concepts, Theories, and Controversies. In *The Handbook of Information and Computer Ethics* (pp. 131–164). John Wiley & Sons.

Tayouri, D. (2015). The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. *Procedia Manufacturing*, *3*, 1096–1100. https://doi.org/10.1016/j.promfg.2015.07.181

Trepte, S., & Masur, P. (2017). *Need for privacy questionnaire (NFP-Q)*. Need for Privacy Questionnaire (NFP-Q). https://www.uni-hohenheim.de/fileadmin/einrichtungen/psych/Dateien/Publikationen/Trepte_Masur_2017_Need_for_Privacy_Questionnaire_NFP-Q.pdf.

Trepte, S., & Masur, P. K. (2020). Need for Privacy. In *Encyclopedia of Personality and Individual Differences* (pp. 3132–3135). Springer.

Tressler, C. (2018, December 26). *Netflix phishing scam: Don't take the bait*. Consumer Information. Retrieved from https://www.consumer.ftc.gov/blog/2018/12/netflix-phishing-scam-dont-take-bait.

Uebelacker, S., & Quiel, S. (2014). The Social Engineering Personality Framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust*. Vienna; IEEE. 10.1109/STAST.2014.12.

Ursachi, G., Horodnic, I. A., & Zait, A. (2015). How Reliable are Measurement Scales? External Factors with Indirect Influence on Reliability Estimators. *Procedia Economics and Finance*, *20*, 679–686. https://doi.org/10.1016/s2212-5671(15)00123-9

US Census Bureau. (2020, October 16). *About Race*. The United States Census Bureau. https://www.census.gov/topics/population/race/about.html.

Venkatesha, S., Reddy, K. R., & Chandavarkar, B. R. (2021). Social engineering attacks during the COVID-19 pandemic. *SN Computer Science*, *2*(2). https://doi.org/10.1007/s42979-020-00443-1

Weirich, D., & Sasse, A. M. (2001). Pretty good persuasion: a first step towards effective password security in the real world. In *NSPW '01: Proceedings of the 2001 workshop on New security paradigms*. ACM. https://doi.org/10.1145/508171.508195.

Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, *59*(2), 431–453.

Wigfield, A., & Eccles, J. S. (2000). Expectancy–value theory of achievement motivation. *Contemporary Educational Psychology*, *25*(1), 68–81. https://doi.org/10.1006/ceps.1999.1015

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*, 412–421. https://doi.org/10.1016/j.chb.2017.03.002

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, *58*(5), 710–722. https://doi.org/10.1002/asi.20530

Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. *CyberPsychology & Behavior*, *11*(5), 615–617. https://doi.org/10.1089/cpb.2007.0208

Yoon, C., Hwang, J. W., & Kim, R. (2012). Exploring Factors That Influence Students' Behaviors in Information Security. *Journal of Information Systems Education*, *23*(4), 407–416. https://aisel.aisnet.org/jise/vol23/iss4/7.

Zeissig, E. M., Lidynia, C., Vervier, L., Gadeib, A., & Ziefle, M. (2017). Online Privacy Perceptions of Older Adults. In *International Conference on Human Aspects of IT for the Aged Population*. Springer, Cham. https://doi.org/10.1007/978-3-319-58536-9_16.

APPENDIX: RESEARCH SURVEY

Introduction

The title of the research project using this survey is "Understanding Susceptibility to Social Engineering Attacks through Online Privacy Behaviors" (IRB #2021-1042). Th purpose of this research survey is to understand the relationship between online privacy behaviors and social engineering attacks. Social engineering attacks can be defined as technical or non-technical attacks that influence people into divulging sensitive information about themselves. Online privacy behaviors can be defined as the steps that an individual takes to protect their personal information by controlling who can see and have access to it.

This survey has a number of questions embedded in it as validity checks to ensure that you are not a robot and are in fact fully reading and answering each question. A unique combination of answers to those questions may result in your survey being rejected.

All your responses to this survey are fully anonymous, and this survey should take you 10-15 minutes to complete. Upon completion of the survey, you will be compensated with $1. If you have any questions, please contact the primary investigator Dr. Ida Ngambeki by email at ingambek@purdue.edu, or Lancia Raja by email at grajaaru@purdue.edu.

Demographics

1. What is your age?

    18-24

    25-34

    35-44

    45-54

    55-64

    65-74

    75 and above

2. What is your gender?

Male

Female

Non-binary/third gender

Prefer not to say

3. What is your ethnicity?

White

Black/African American

American Indian or Alaska Native

Asian

Native Hawaiian or Pacific Islander

Prefer not to say

Other (please specify)

4. What is the highest degree or level of schooling that you have completed? (If you are currently enrolled, select highest degree received prior to enrollment)

No level of school completed

Elementary to 8th grade

High school, no diploma

High school graduate, diploma or equivalent

Associate degree

Bachelors' degree

Masters' degree

Doctorate/Professional degree

Prefer not to say

Social Engineering Victimization

5. Have you ever been a victim of one or more of the following social engineering attacks? (Select all that apply)

Phishing (Attack that aims to gain confidential information fraudulently through emails)

Smishing (Attack that aims to gain confidential or sensitive information via text messages)

Pharming (Attack that aims to gain confidential information through fake websites or webpages)

I have not been a victim of these social engineering attacks

6. Have you ever suffered serious consequences as a result of a social engineering attack? (Example – financial losses, compromise of personal information)

Yes

No

I have not been a victim of social engineering attacks

7. How susceptible do you believe you are to social engineering attacks?

Not at all susceptible

Slightly susceptible

Moderately susceptible

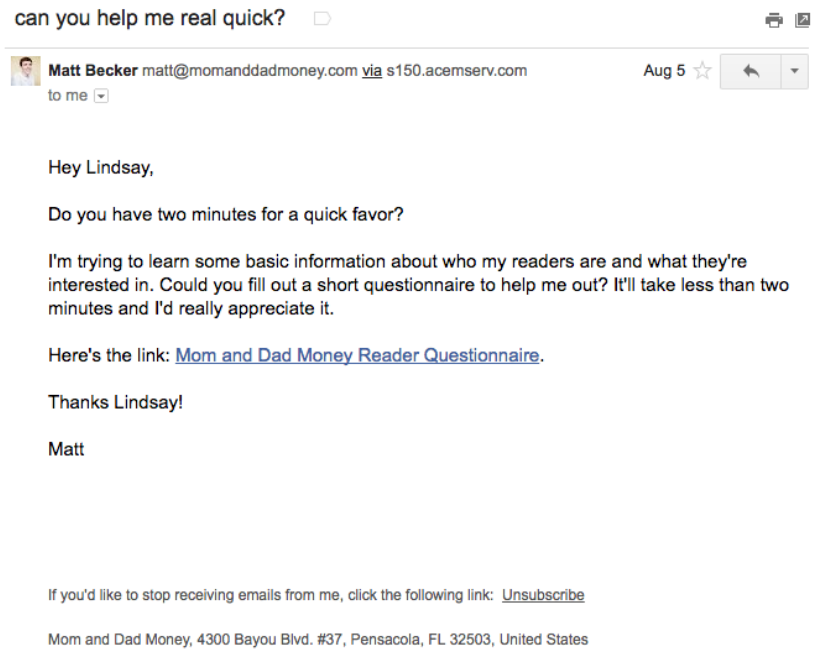
Very susceptible

Extremely susceptible

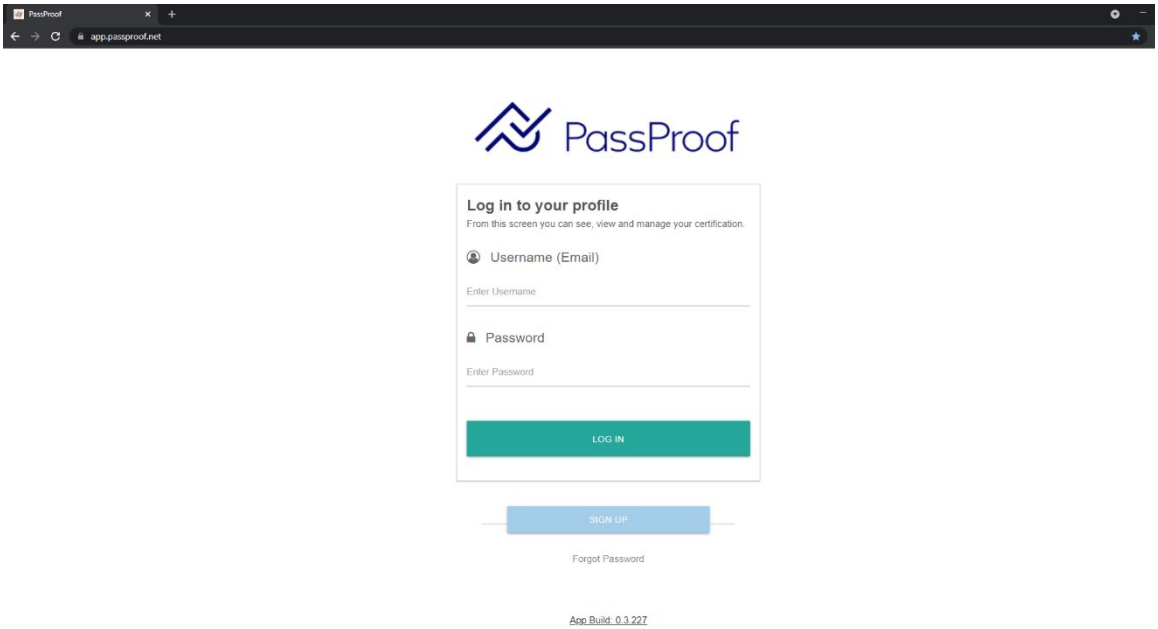
Social Engineering Susceptibility

In this section, you will be presented with some scenarios in the form of screenshots. Please indicate the extent to which you are confident that the scenario is a social engineering attack. (Items are scored on a 5-point Likert scale, ranging from "Extremely confident" to "Not confident at all")

1. How confident are you that this scenario is a social engineering attack? (Cox, 2021)

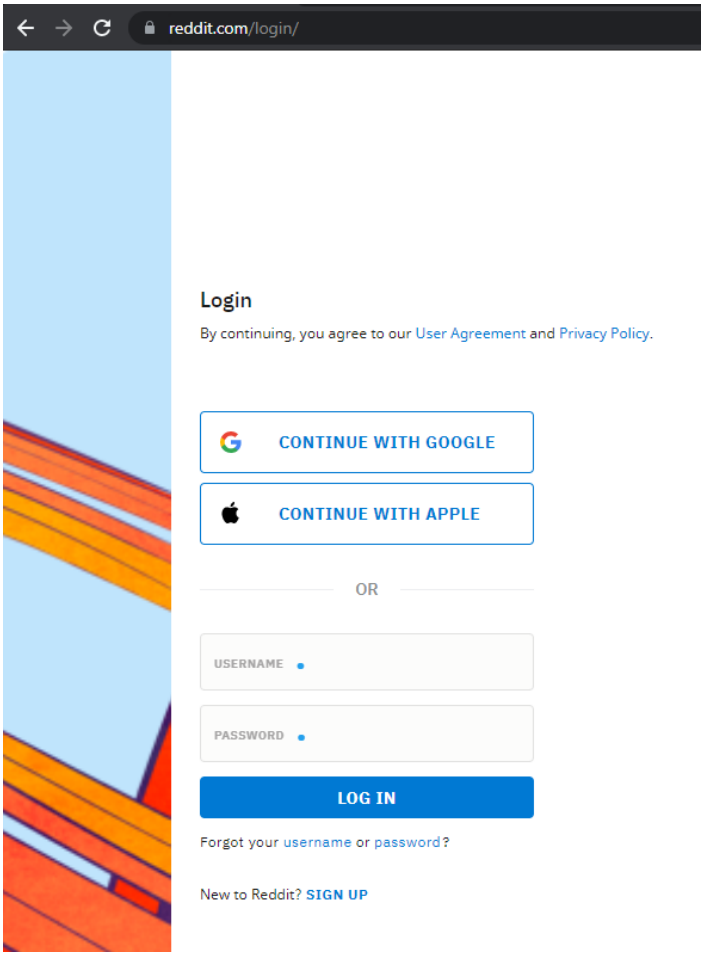


2. *How confident are you that this scenario is a social engineering attack? (PassProof, 2020)*

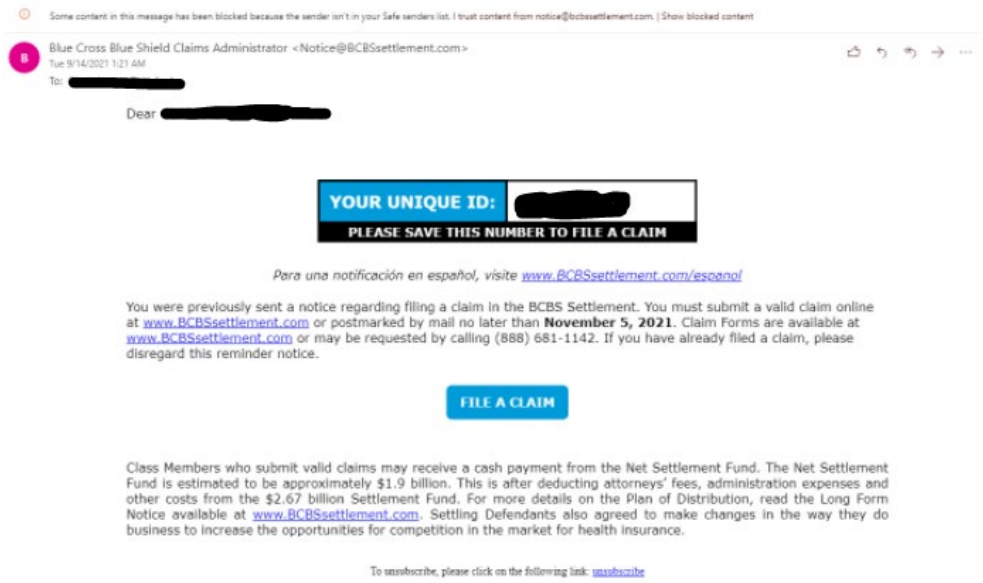


3. *How confident are you that this scenario is a social engineering attack?*

4. *How confident are you that this scenario is a social engineering attack? (Reddit, 2021)*



5. *How confident are you that this scenario is a social engineering attack?*


Some content in this message has been blocked because the sender isn't in your Safe senders list. I trust content from notice@bcbssettlement.com. | Show blocked content

Blue Cross Blue Shield Claims Administrator <Notice@BCBSsettlement.com>
Tue 9/14/2021 1:21 AM
To: [redacted]

Dear [redacted]

YOUR UNIQUE ID: [redacted]
PLEASE SAVE THIS NUMBER TO FILE A CLAIM

Para una notificación en español, visite www.BCBSsettlement.com/espanol

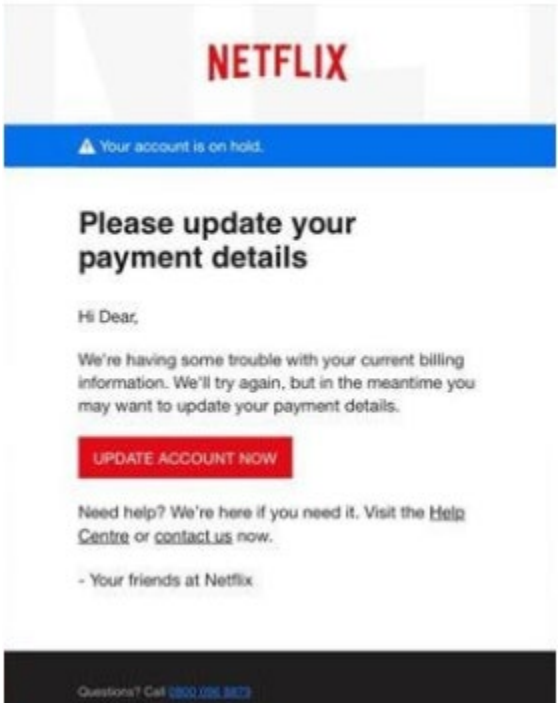
You were previously sent a notice regarding filing a claim in the BCBS Settlement. You must submit a valid claim online at www.BCBSsettlement.com or postmarked by mail no later than **November 5, 2021**. Claim Forms are available at www.BCBSsettlement.com or may be requested by calling (888) 681-1142. If you have already filed a claim, please disregard this reminder notice.

FILE A CLAIM

Class Members who submit valid claims may receive a cash payment from the Net Settlement Fund. The Net Settlement Fund is estimated to be approximately $1.9 billion. This is after deducting attorneys' fees, administration expenses and other costs from the $2.67 billion Settlement Fund. For more details on the Plan of Distribution, read the Long Form Notice available at www.BCBSsettlement.com. Settling Defendants also agreed to make changes in the way they do business to increase the opportunities for competition in the market for health insurance.

To unsubscribe, please click on the following link: unsubscribe

6. *How confident are you that this scenario is a social engineering attack? (Tressler, 2018)*


NETFLIX

Your account is on hold.

Please update your payment details

Hi Dear,

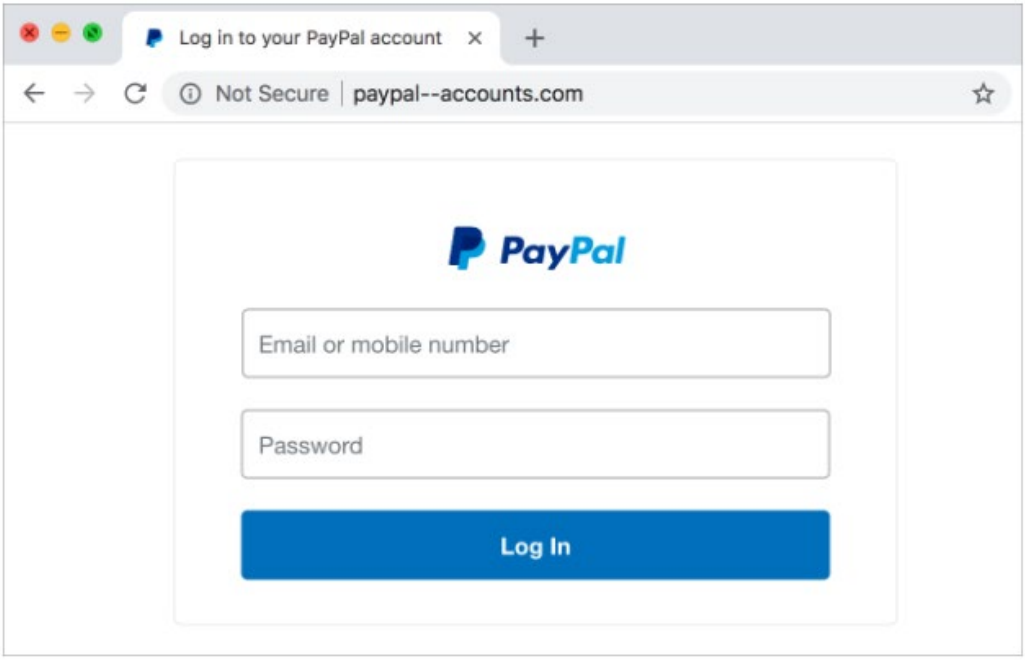
We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

UPDATE ACCOUNT NOW

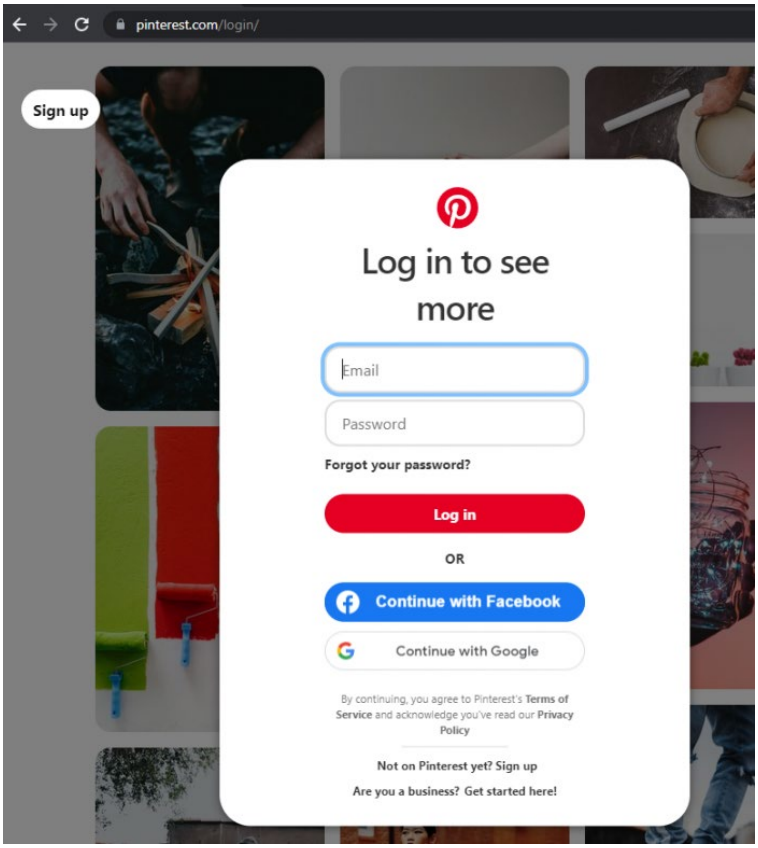
Need help? We're here if you need it. Visit the Help Centre or contact us now.

- Your friends at Netflix

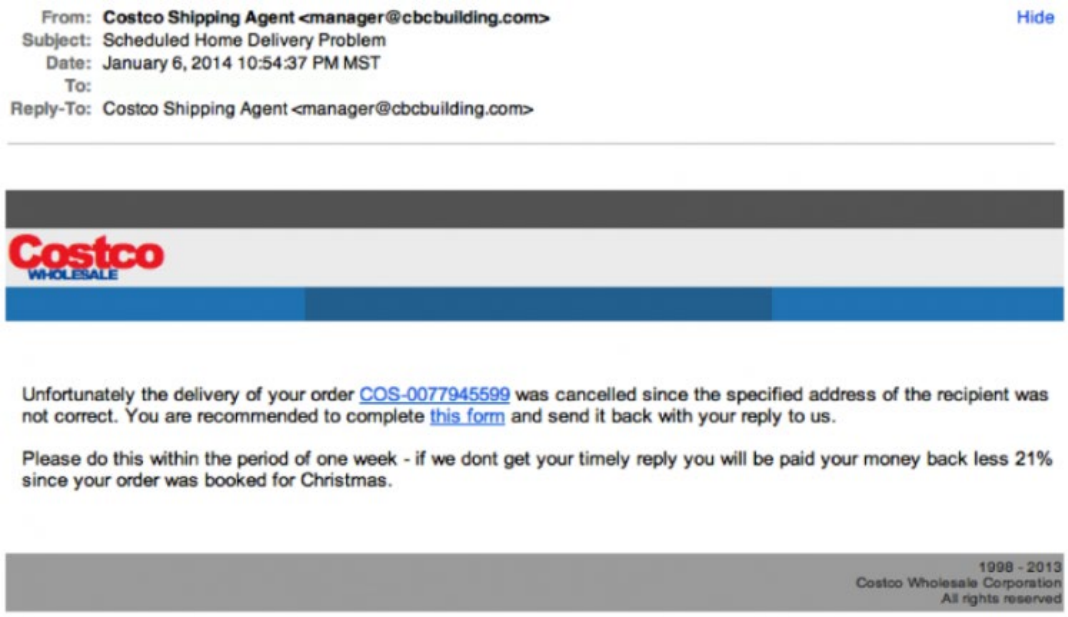
7. *How confident are you that this scenario is a social engineering attack? (Fox, 2020)*



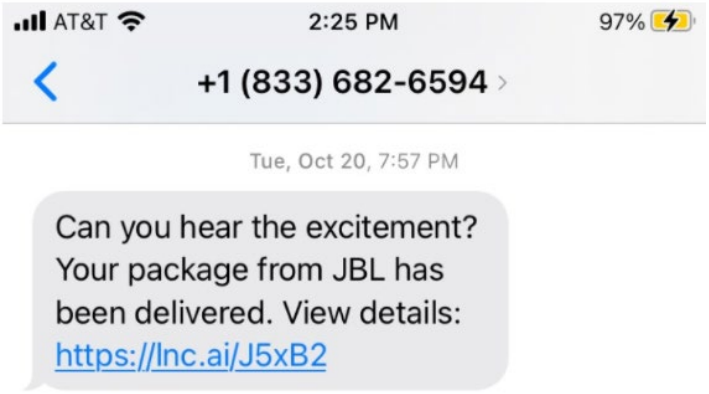
8. *How confident are you that this scenario is a social engineering attack? (Pinterest, 2021)*



9. *How confident are you that this scenario is a social engineering attack? (Ellis, 2021)*



10. *How confident are you that this scenario is a social engineering attack?*



11. *Select the word "Nine" from the following options*

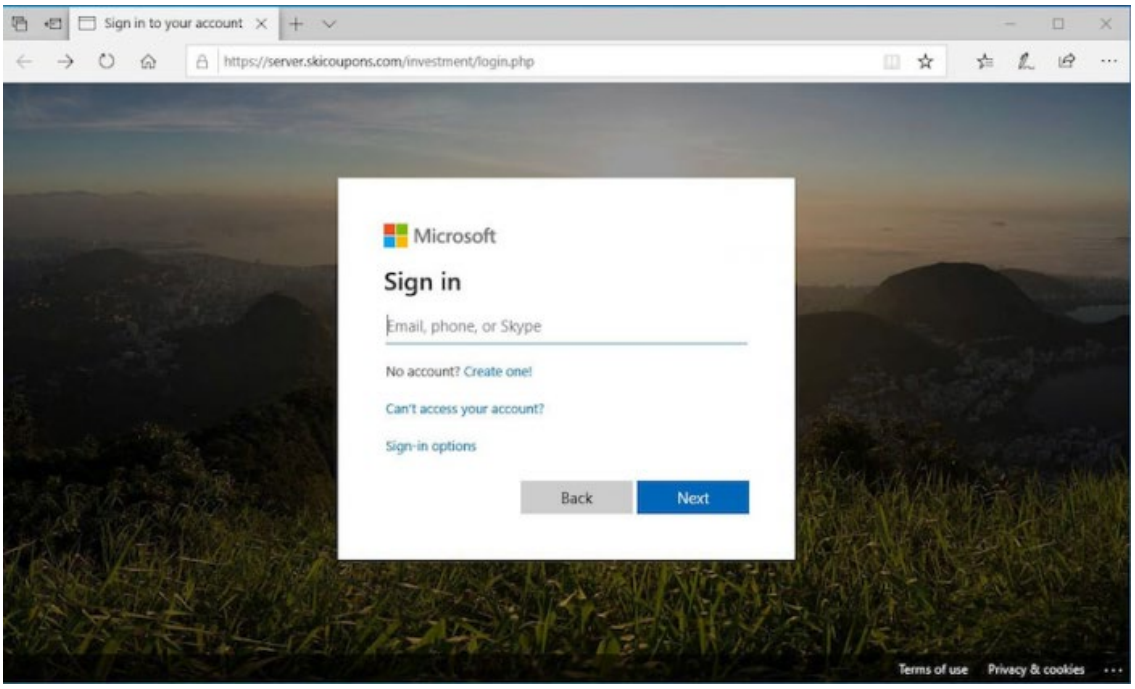
Seven

Ten

Six

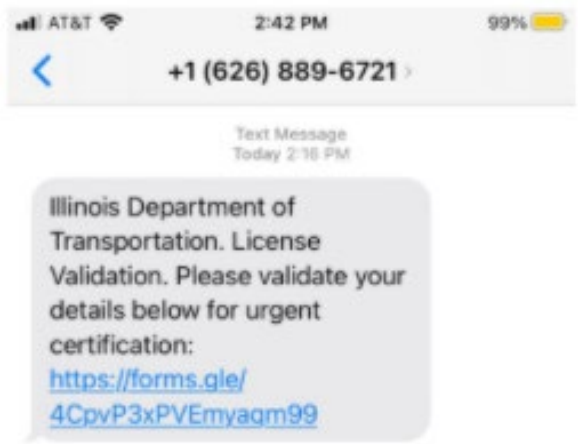
Nine

12. *How confident are you that this scenario is a social engineering attack? (Bit Sentinel, 2020)*

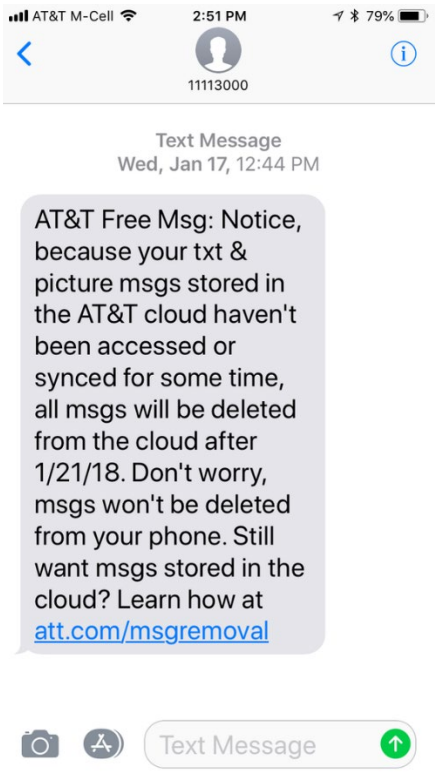


13. *How confident are you that this scenario is a social engineering attack? (Krebs, 2017)*

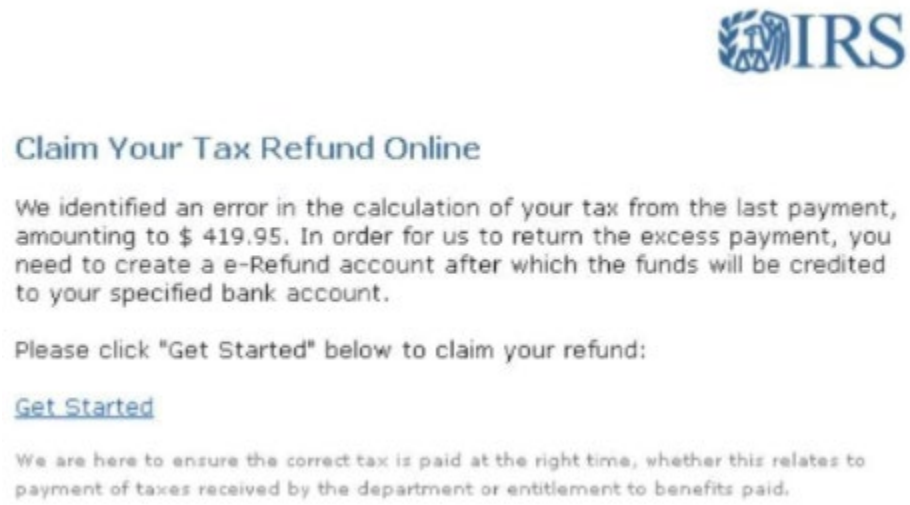
14. *How confident are you that this scenario is a social engineering attack?*



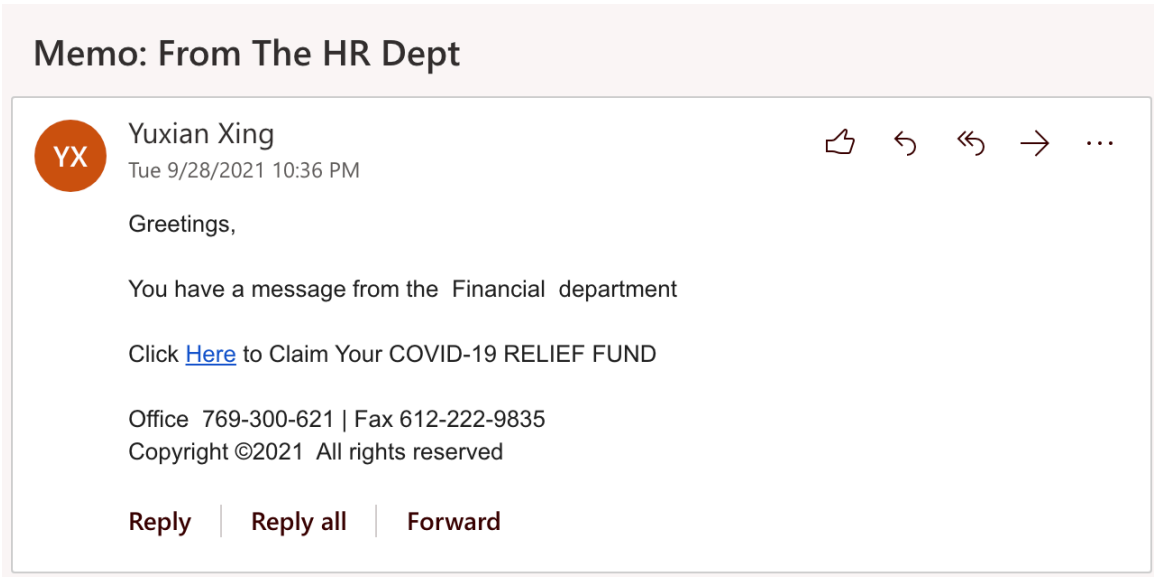
15. *How confident are you that this scenario is a social engineering attack? (AT&T, 2018)*



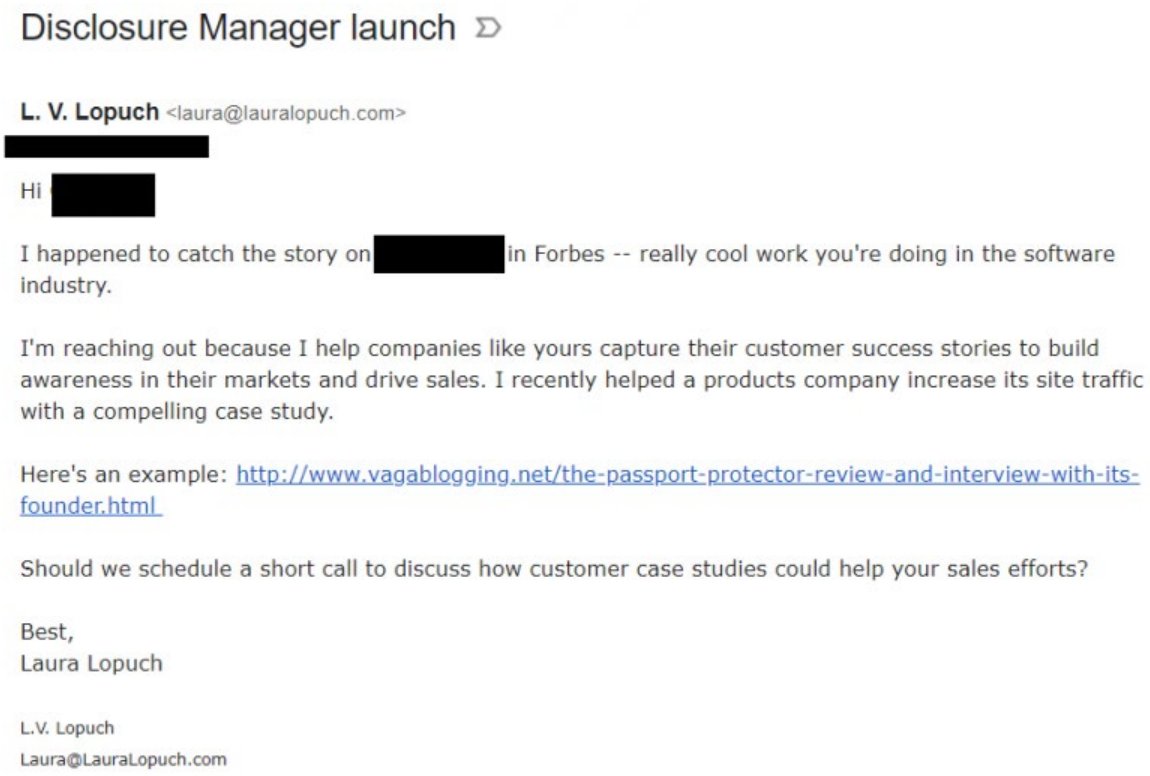
16. *How confident are you that this scenario is a social engineering attack? (Rafter, 2020)*



17. *How confident are you that this scenario is a social engineering attack?*



18. *How confident are you that this scenario is a social engineering attack? (Lopuch, 2021)*



Disclosure Manager launch

L. V. Lopuch <laura@lauralopuch.com>

[redacted]

Hi [redacted]

I happened to catch the story on [redacted] in Forbes -- really cool work you're doing in the software industry.

I'm reaching out because I help companies like yours capture their customer success stories to build awareness in their markets and drive sales. I recently helped a products company increase its site traffic with a compelling case study.

Here's an example: http://www.vagablogging.net/the-passport-protector-review-and-interview-with-its-founder.html

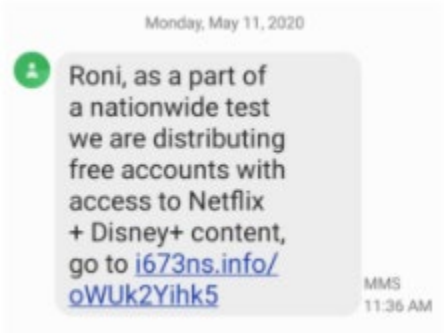
Should we schedule a short call to discuss how customer case studies could help your sales efforts?

Best,
Laura Lopuch

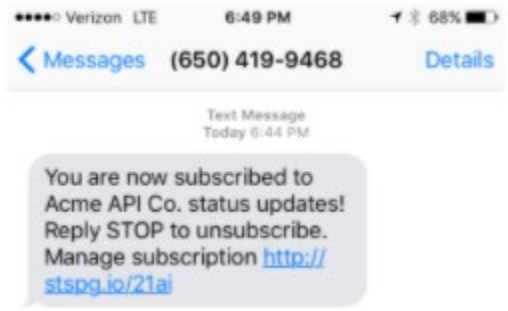
L.V. Lopuch
Laura@LauraLopuch.com

19. *How confident are you that this scenario is a social engineering attack? (ProofPoint, 2021)*

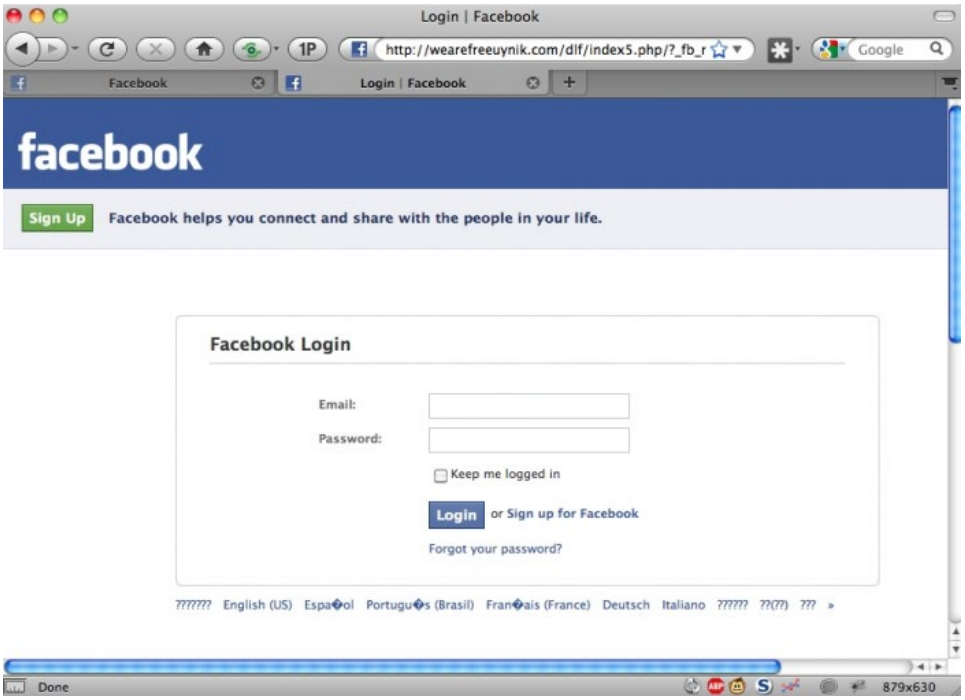
20. *How confident are you that this scenario is a social engineering attack? (Crane, 2020)*



21. *How confident are you that this scenario is a social engineering attack? (Atlassian, 2020)*



22. *How confident are you that this scenario is a social engineering attack? (Bit Sentinel, 2020)*



Need for Privacy (Trepte & Masur, 2017)

Please indicate the extent to which you agree with the following statements (*Items are scored on a 5-point Likert scale, ranging from "Strongly disagree" to "Strongly agree")*

1. I prefer that not much is known about me.

2. I prefer to remain unrecognized.

3. I do not want my personal data to be publicly available.

4. Not everyone needs to know everything about me.

5. I do not like to stand in a densely packed crowd.

6. I do not like to sit next to a stranger on the bus or tube.

7. I do not like it when strangers come too physically close to me.

8. I do not like it when other people enter my house or my room unannounced,

9. It is hard for me to talk about myself

10. I feel uncomfortable when others share private information about their lives.

11. There are many things about me that I do not want to discuss with other people.

12. I prefer not to talk about personal things unless my conversational partner brings them up first.

Privacy Self-Efficacy (Zeissig et al., 2017)

Please indicate the extent to which you agree with the following statements (*Items are scored on a 5-point Likert scale, ranging from "Strongly disagree" to "Strongly agree")*

1. I know most privacy settings of the applications I use.

2. Because I have had no problems with privacy settings so far, I am confident for future privacy tasks.

3. I do not read privacy policies because I do not understand them.

4. I always change my privacy settings when I start using a new device.

5. I always change my privacy settings when I start using a new application.

6. I feel helpless with privacy settings and measures, so I do not change anything.

Response Efficacy (Boerman et al., 2018)

Please indicate the extent to which you agree with the following protective behaviors being effective against collection, usage and sharing of personal information on the internet (*Items are scored on a 7-point Likert scale, ranging from "Strongly disagree" to "Strongly agree")*

1. Installing an ad-blocker

2. Deleting cookies

3. Declining to accept cookies

4. Usage of private mode in a browser

5. Deleting browser history

6. The usage of opt-put websites to configure whether ads are based on personal online behavior

7. Activating the “Do Not Track” function in a browser

8. The usage of special software in a browser (such as Ghostery and AbineTaco) that makes it harder companies to collect personal information

9. Filling out wrong information about yourself (such as a fake name or wrong email address) when asked for such information

Privacy Protective Behaviors (Boerman et al., 2018)

(The items were scored on a 6 point scale as follows: 1 = Never, 2 = Rarely, 3 = Occasionally, 4 = Often, 5 = Very Often, 6 = Do Not Know)

1. How often do you use an ad blocker?

2. How often do you delete cookies?

3. How often do you decide to refrain from visiting a website because it is only accessible when you accept cookies?

4. How often do you decline to accept cookies when the website offers the choice?

5. How often do you use the private mode in your browser?

6. How often do you delete your browser history?

7. How often do you use opt-out websites (such as www.youronlinechoices.com) to configure whether ads are based on personal data?

8. How often do you use the "Do Not Track" function in your browser?

9. How often do you use special software in your browser (such as Ghostery and AbineTaco) that makes it harder for companies to collect personal data?

10. How often do you fill out wrong information about yourself (for instance, a fake name or wrong email address) when asked for such information?

11. How often do you read the terms and conditions page of an online application or service that you use?

12. How often do you accept friend requests from strangers across online networking applications?

13. How often do you limit the amount of personal information that you post online (examples - current location, achievements, information about family members)?

14. How often do you use a virtual private network (VPN)?