EXPLORING PHISHING SUSCEPTIBILITY ATTRIBUTABLE TO AUTHORITY, URGENCY, RISK PERCEPTION AND HUMAN FACTORS

by

Priyanka Tiwari

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
August 2020

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Ida Ngambeki, Chair

Department of Computer and Information Technology

Dr. John Springer

Department of Computer and Information Technology

Dr. Baijian Yang

Department of Computer and Information Technology

Approved by:

Dr. John Springer

I dedicate my thesis to my dear parents, supportive brother, my late grandfather Mr. Anand Shankar Tiwari, extended family and kind friends, who supported me and believed in me throughout my Master study. Special thanks to my advisor Ida Ngambeki for guiding me through the field of behavioral cybersecurity and inspiring me with new ideas.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

SE	Social Engineering
ARPANET	Advanced Research Projects Agency Network
ASE	Automated Social Engineering
IDS	Intrusion Detection Systems
VOIP	Voice Over IP
SEPF	Social Engineering Personality Framework
ELM	Elaboration Likelihood Model
SCAM	Suspicion, Cognition and Automaticity Mode

ABSTRACT

Security breaches nowadays are not limited to technological orientation. Research in the information security domain is gradually shifting towards human behavioral orientation toward breaches that target weaknesses arising from human behaviors (Workman et al., 2007). Currently, social engineering breaches are more effective than many technical attacks. In fact, the majority of cyber assaults have a social engineering component. Social Engineering is the art of manipulating human flaws towards a malicious objective (Breda et al., 2017). In the likely future, social engineering will be the most predominant attack vector within cyber security (Breda et al., 2017). Human failures, persuasion and social influences are key elements to understand when considering security behaviors. With the increasing concerns for social engineering and advancements in human factors-based technology, phishing emails are becoming more prevalent in exploiting human factors and external factors. Such factors have been researched upon in pairs, not overall. Till date, there is not much research done to identify the collaborative links between authority, urgency, risk perception and human factors such as personality traits, and knowledge. This study investigates about phishing email characters, external influences, human factors influences, and their collaborative effects.

Keywords: Social Engineering attacks; Cyber Security; Personality Traits; Social Engineering; Phishing; Spear phishing; Social Engineering Personality Framework; Authority; Urgency; Risk Perception; Cyber knowledge; Elaboration Likelihood Model; The suspicion, cognition and automaticity mode; Human factors; User susceptibility

CHAPTER 1. INTRODUCTION

1.1 Introduction

"Social engineering is lying, it just sounds better than saying you are a liar" (Cole et al., 2005). Nowadays, social engineering is becoming ubiquitous due to its human-factor based vulnerability exploitation which can be both cheap and effective, and the limitations it exploits in technical security. Administrators today are becoming as concerned with social engineering as with technical attacks when it comes to security. However, social engineering attacks are difficult to detect. Kevin Mitnick highlighted this after attending RSA conference in 2001:

> "No sessions were offered covering physical attacks or social engineering. You could spend a fortune purchasing technology and services from every exhibitor, speaker and sponsor at the RSA Conference, and your network infrastructure could still remain as vulnerable to old-fashioned manipulation"

With today's advancements in network security, humans are now classified as the weakest link in the procedure. Attackers strategize their attacks and targets the weakest link in the security chain with the expectations of acquiring the most information, thereby, imposing the most damage. Technical barriers such as firewalls, routers and other safeguards are insignificant if an invader can physically gain access. With the advancement in machine learning techniques, new algorithms and models are being created and directed to understand human factors involved in social engineering. But the lack of psychological understanding in these techniques presents a major loophole. This loophole opens up possibilities to exploit behavioral and psychological weaknesses to compromise security.

Phishing, or web spoofing, is a rising issue. The Anti-Phishing Working Group (APWG) reports that starting in mid-March 2020, cybercriminals stimulated a variety of COVID-19 themed malware and phishing attacks against workforces, healthcare services, and the newly out of work population. Phishing sites detected in the first quarter of 2020 was 165,772, which went up from the 162,155 observed in the fourth quarter of 2019. Phishing attacks do sound work by aiming for a user's incapability to differentiate genuine sites from spoofed ones. Majority of the prior research emphasizes on supporting the user in making this discrepancy; though, users must head for the right security choice every single time. Regrettably, humans are less proficient to perform the security investigations essential for legitimate secure site recognition, and a single error may cause full loss of user's online account. For financial organizations, phishing is a predominantly deceiving problem, as trust is the basis for customer associations and relationships, and phishing incidents weaken belief in an organization. Behavioral and contextual factors of the user, when manipulated, could result in susceptibility to phishing. Such factors when combined with principles of influence can lead users further prone to phishing as these factors are human-borne and can be manipulated.

In this literature review, we discuss social engineering, its historical context, nature, and its impact. Later, we describe the mechanisms of social engineering including persuasion. Next, we explore theories of persuasion and their components. We then describe cognitive models used in decision making processes such as ELM, SCAM. Next, we elaborate over email cues taking authority, urgency, risk factors that provide central and peripheral routes to phishing. Later, we describe argumentation scheme, message framing. We then describe personality traits, and its relationship with persuasion, social engineering. Then, we proceed towards the social engineering personality framework which explains the association in personality of social engineer and victim. Afterwards, we dig deep in spear-phishing and its association with personality, internet usage, and explore its application in financial sector. We then discuss the limitations with phishing research in the area of integrated study of such factors.

1.2 Statement of the problem

This experiment explores the effect of contextual and human factors including urgency, personality traits, knowledge, risk factors, persuasion principle that affect the users' susceptibility for phishing emails. The method will take personality traits into consideration and will examine whether authority-based spear phishing attack affects victims and the involvement of authority, urgency, risk factors, and other human factors such as knowledge as the influencing measures for the likelihood of falling for phishing emails.

From previous research, we conclude that using authority as per victims' personality traits for spear phishing attacks is correlated and produce profound effect on victims' side. It is crucial to understand the involvement and impact of urgency, authority, risk factors and human factors on victims.

This research concentrates on the varying effect of authority, urgency, risk, personality traits, knowledge influence on phishing victims with various personality traits.

1.3 Research questions

RQ1. Does presence of authority and cues within phishing emails affects the likelihood of responding to phishing emails?

RQ2. Does presence of risk perception affect the likelihood of responding to phishing emails?

RQ3. Does falling victim to phishing emails previously affect the likelihood of responding to phishing emails?

RQ4. Do personality traits affect the principles of influence when responding to phishing emails?

1.4 Hypothesis

H1. Authority is related to conscientiousness and agreeableness
H2. Urgency is related to extraversion and openness
H3. People who were victims of phishing are more likely to be influenced by authority
H4. People who were victims of phishing are more likely to be influenced by urgency
H5. People who were victims of phishing are more likely to be influenced by risk
H6. Authoritative emails are more likely to result in clicks
H7. Emails containing urgency language are more likely to result in clicks
H8. Emails that require actions posing greater risk will be less likely to be clicked
H9. Authority and urgency interact to affect users' susceptibility to phishing email
H10. Authority, urgency, and risk interact to affect users' susceptibility to phishing email

1.5 Scope

The purpose of this study is to understand the effect of authority, urgency, risk factors and human factors on users' susceptibility towards phishing email. This would involve finding a way to understand the effects of authority-based principles of persuasion, urgency, risk factors, personality traits, and its relative effects on victims with various personality traits.

1.6 Significance

With the speedy growth of the internet and availability of information, social engineering attacks are majorly becoming common. Authority based spear phishing attacks are becoming quite popular as it mostly targets victims with specific intentions. Since the personality traits of victims also provide various possibilities from an attacker's side to manipulate the information in hand, personality traits in particular hold an abstract point of view for attack. Messages/script can be altered with several human behavioral and contextual factors to serve the purpose of manipulating victim.

To the best of our knowledge, the subsequent work in this study will be based on understanding the effects of authority, urgency, risk perception, personality traits, human factors affecting users through phishing emails.

1.7 Assumptions

This study work on the following assumptions:

- Limiting principle of persuasion used by social engineer to authority, urgency and related measurement in potential victim.
- Behavioral intention to act on potentially phishing emails is a reasonable proxy for behavioral action.

1.8 Limitations

The study is undertaken with the following limitations:

- The study relies on self-reported data so it may be subject to response bias
- The study population was recruited from a particular on-demand platform (i.e., Amazon Mechanical Turk). MTurk population is generally limited and certainly overused, and the targeted groups representing certain behaviors are underrepresented and hard to be considered over such platforms (Chandler et al., 2019)

CHAPTER 2. LITERATURE REVIEW

This chapter is a summary of the recent research in social engineering, persuasion, personality traits, principle of influence, phishing and risk perception of victims.

2.1 Social engineering defined

With the mark of the digital age, massive amounts of data are abundantly available and securing data has become a major concern. The majority of researchers concentrate on improving the technical facets of security. The human component - the weakest link (Schneier, 2006), is often overlooked. Attacks targeting the human element of security are called social engineering. It is essentially the art of persuasion – influencing users to reveal sensitive data or carry out some action. Social engineers try to get access to classified information by exploiting the human component of security. Social engineers' prey on the qualities of human nature, such as the assumption that one can trust strangers, general courtesy, the desire to be helpful to others, or the desire for quick and easy rewards. It generally occurs in four phases: i) reconnaissance (where the attacker gathers relevant information about the target and identifies how it can be used), ii) developing a relationship (the attacker tries to gain the trust of his target for easy manipulation), iii) exploitation (attacker tries to influence his target into exposing information or executing a certain action) iv) execution (Breda et al., 2017).

2.2 History of social engineering research

2.2.1 Preexistence in politics

The first occurrence of the term "Social engineer" dates back to 1842 in the book titled "An efficient Remedy for the distress of Nations" written by the famous British economist John Gray. In 1914, the great American social worker, social reformer and activist – Jane Addams, employed "social engineering" for the policies of labor exchanges and social insurance efforts by European government to battle unemployment (Addams, 1914).

By 1929, the "social engineering" concept was being applied to legal professions (Slade, 1929, 213). During 1937, Joseph S. Davis of Stanford University backed the idea of a new academic discipline of "social engineering" relevant to social scientists. This enabled social scientists to process and understand social statistical data with latest social scientific techniques (Davis, 1937). Davis claimed that social engineers, like doctors, have the expert knowledge essential to manipulate society in several ways – spinning and playing around with the social and economic factors till the preferred outcomes.

2.2.2 Cyber age concerning social engineering

Computational devices existed since the era of Charles Babbage (1791-1871) although they were not in commercial use. "Cyber age" not only denotes usage of computational devices, but a network of such interconnected computational devices. Such network computing immediately brings security concerns.

"Social engineering" began with the "phone phreaking" spectacle of the late 1950s, which existed before the creation of ARPANET. These initial developments shaped the social engineering contexts. Before phone phreaking, the term "social engineering" had specifically been applicable to the activities of commanding policy organizers – folks in government or business attempting to treat what they identified as "social harms" using their exclusive practical intelligence (Hatfield et al., 2018).

In 1984, the early hacker magazine 2600: The Hacker Quarterly published the term "social engineering" in an anonymous article. By 1990, the technical terrain grew in popularity and as a research topic, paving the way for information gathering through impersonation and manipulation to be easier. The quality of information had risen dramatically. Such information could then aid attacks directly without caring about technical details and manipulating such information. Certainly, viewers now refer to social engineering as "the peak form of hacking" (Greiner, 2006).

2.2.3 Social engineering now

With increased eminence of social engineering attacks, there has been rise in application of core principles of social engineering including behavior and susceptibility of users (Cialdini, 2001, Gragg, 2003, and Stajano et al., 2011). Such efforts revised the perceptions of psychology to recognize aspects that builds the possibility of a social engineer's accomplishment when deceiving a human victim. Individuals are inclined towards believing that the people/organizations they perceive as amiable have been recognized as authoritative bodies.

With the growth of Automated Social Engineering (ASE), artificial intelligence, and machine learning, technical descriptions will no longer be adequate to clarify aspects of social engineering that go out of the reach of human contact. The usage of automated bots, altering social media environments without human interventions, is already creating extreme impact on social engineering (Huber et al, 2011, Jhaveri et al., 2014). Future of automated social engineers holds identifying and automating targeted attack by adapting latest automated attack strategy empowered by machine learning. Identifying behavioral aspects of humans online is one part of automated social engineer and it is gaining popularity in research area.

2.3 Nature of social engineering attacks

The common essence of social engineering is that it involves methods that can control human behavior. Social engineers can manipulate victim’s behavior by inducing strong human emotions. An attacker uses a credible story to provoke the trust of the victim. Such stories used in such circumstances urges to elementary human natures like hate, greed, fear, or compassion. Attackers usually advance trust by insistently urging the victim to link to such sentiments.

2.4 Impacts of social engineering

Every single social engineering attack is linked with an end goal. The goal can take any form, be it serious issues such as getting privileged file system access of the company’s network to less critical problems like tailgating etc. Attacker often deploys an attack plot at various points of the process in the direction of the objective. Even though the worth of the information obtained might not be huge, every occurrence of an invader accomplishing what he or she wants through social engineering means can be an effective attempt (Thornburgh, 2004). It is frequently the collective effect of the success of numerous such attacks that the attacker is eventually after. Hence, social engineering methods are not essentially a one-step attack or a means to a closure (Ivaturi et al., 2011).

2.5 Mechanisms of social engineering

2.5.1 Persuasion

According to Cialdini, 1993, persuasion is human interaction formulated to vary the intuitive decisions and spontaneous actions of others. Persuasion is a procedure of attempted impact as it looks for altering the way others perceive, think, or act. Cialdini, 1993 categorizes his group of influence principles as: (1) contrast, (2) reciprocity, (3) consistency, (4) social proof, (5) authority, (6) liking, and (7) scarcity. These perceptive types are specially needed when people don’t have the leaning or means to involve in more alert message processing.

2.5.2 Persuasion and social engineering

In the perspective of social engineering attacks, authority (63%) shows the highest effectiveness (Bullée et al., 2018). Authority, compared to other persuasion techniques, is used considerably more often than others. Persuasion principles when compared to other social influences, is more often used. Security mechanisms should not be limited to technical countermeasures, but also social countermeasures should be deployed.

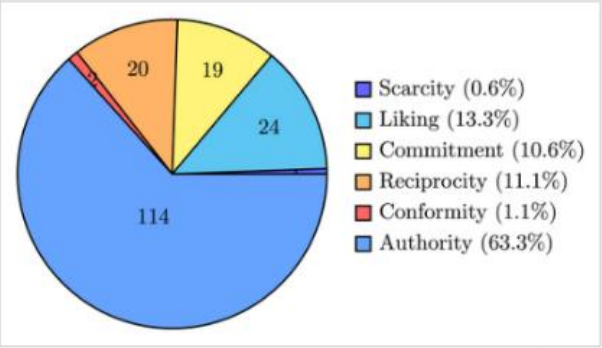


Figure 1. Persuasion principles used (Bullée et al., 2018)

During a social engineering attack, effects of authority plays a prime role. Authority, one of the six principles of persuasion, when employed for an intervention-based study, presented the results as those who were exposed to intervention before were able to identify the social engineering attack while those who were not, most of them succumbed to giving away the keys to the social engineer who played as authority (Bullée et al., 2015).

2.6 Cognitive procedures in decision making process

This section investigates the cognitive procedures users generally engage into critic phishing emails and rationalize their consecutive actions. This is important for recognizing weaknesses in user's decision-making process that direct them to answer to phishing emails.

In previous researches, investigators have taken steps to identify the elementary factors that may influence users' susceptibility to phishing emails. This led to enrichment in progress and implementation of a sequence of theoretical frameworks, involving Protection Motivation Theory (PMT; Rogers, 1975), Elaboration Likelihood Model (ELM; Petty et al., 1986), and the Suspicion, Cognition, and Automaticity Model (SCAM; Vishwanath et al., 2018). Such models have hardly been studied together, even though these models display a degree of intersection and the factors involved are expected to influence users' susceptibility to spear phishing. For example, the SCAM model consists of individual's beliefs, knowledge and behaviors with respect to phishing susceptibility precisely. On the contrary, Protection Motivation Theory has wide application in general security behavior and inspects user's perceptions of self-efficacy and severity of threat. These models have also not been widely studied using dataset with responses to hierarchical based dataset with varying authority power. Exploring the part of all of these characteristics within hierarchical situations offers an exclusive chance to understand the full variety of features that may impact susceptibility of users. We now describe ELM and SCAM models with respect to our study.

2.6.1 Elaboration Likelihood Model (ELM)

Elaboration Likelihood Model (Petty et al., 1986) is a "well-known dual-process theory of information processing on persuasion". Research studies involving persuasion show how user's attitudes can change with the received emails/messages. The thought of the dual-process theories works on the principle that when being influenced, people must initially determine the legitimacy and soundness of the received message. Adding to the information processing of the content of the message, people also look into the features neighboring the messages. In ELM, central route makes up the persuasion through information content: people detail over the message and cautiously and considerately assess the soundness of the message's content (Petty et al., 1986). Any other persuasion that does not detail over message comes under peripheral route (Eagly et al., 1993). Classically, peripheral routes take lead of the cues surrounding the message – such as credibility, authenticity and message length – to conclude message's validity (Petty et al., 1986).

Peripheral route is dependent on the heuristic cues that are promptly available and commonly used. Source credibility is one of the most extensively studied heuristic cue (Sussman et al., 2003; Zhang et al., 2008) and exploited by phishing criminals. Phishing messages pretend to come from trustworthy and reliable sources such as authoritative divisions, trustworthy businesses. The success of such forged source credibility has been frequently used in actual phishing attacks.

Traditional phishing approaches using credibility potently stress on authority. The Oxford English Dictionary (1989) defines authority as "derived or delegated power; conferred right or title; authorization". Such credible authoritative sources vouch in to gain piece of information.

As per ELM, the degree of elaboration varies with the neighboring context. ELM uses elaboration likelihood term to understand and get the probability of people taking the central route and the range of such elaboration (Petty et al., 1986). Whether user take the central route or not is highly influenced by their elaboration likelihood for information. Numerous aspects are identified to influence elaboration likelihood, involving personality traits, contextual factors such as users' expert knowledge and involvement (Petty et al., 1986). Such variables act in two ways: by disturbing one's inspiration to involve in elaboration and/or by changing one's aptitude to participate in elaboration.

When ELM is applied to phishing, it offers the tool that can define and clarify the located roles played by several factors. Workman et al., 2008 successfully argued that reduction in elaboration likelihood of users can be due to personality traits such as inclination towards trust and establishing commitment. Vishwanath et al., 2011 presented that peripheral processing was the leading processing mode responsible for phishing victimization and message urgency, its source, and composition elements served as peripheral cues when involved with phishing susceptibility.

To our knowledge, the relative role of credibility (especially authority), urgency and personality traits serving as peripheral cues has yet to be studied explicitly within hierarchical settings. In our study, we investigate whether the existence of urgency, authority and personality traits influence users' susceptibility to phishing emails.

2.6.2 The suspicion, cognition and automaticity mode (SCAM)

The SCAM states that individual user characters (Vishwanath et al., 2018) regulate the degree to which heuristic processing approaches are used while assessing emails (Vishwanath et al., 2018). Such variances mainly tell about user beliefs concerning online risk (Barnett et al., 2001, Bromiley et al., 1992), including the level of experience, efficacy, and expert knowledge people have (Downs et al., 2007, Canfield et al., 2016). But the association among these factors remain unidentified. Henceforth, users possessing greater mindfulness or risk based experience of online activities are more probable to be involved in deeper information processing within emails. Contrarywise, users with a lower alertness are considered further likely to be involved in heuristic forms of information processing.

However, it is not clear up to what extent such concepts apply to the simulated spear-phishing emails. For instance, the degree of influence of training approaches in order to lessen employee susceptibility remains undefined (Caputo et al., 2014).

Within our study, we investigate the possible role of risk factor and previous knowledge, that is, if someone has previously fallen victim to a phishing email and the corresponding learning curve.

2.7 Email Cues

Difficulty in detecting and identifying phishing attacks tells a lot about how users perceive and puts up the effort in identifying phishing attacks. The general detection procedure includes identifying cues that determines if an email or website is legitimate or not (Rui et al., 2020); for instance, noticing safety indicators such as checking URL's authenticity, graphical cues like logos, images, authority's seal and domain name (Dhamija et al., 2006); and then utilizing such cues to claim the authenticity, evaluate them and arrive to a global consent for such phishing emails. In the past, the phishing detection process has been examined with studies either focusing on the factors that lead users to fall victim to phishing attacks, or the impact of training on those factors. Identifying and marking emails as phishing requires a detection procedure which will be directly related to the varying difficulty level in the identification process. Such cues, once identified, are then used for designing and developing training programs concentrating to lower victimization rates. Detection process can have one or multiple stages which user might perceive as problematic to follow. Such complicated navigation won't do any good to user's lack of ability and users will remain prone to be victimized by phishing emails.

Very few studies have focused on examining the collaborative effects of multiple influence principles in the same research. Results of Parsons et al., 2019 showed that observers in the study were more susceptible to social proof and scarcity principles of influence and least susceptible to authority principle. Though, in an email, participants may have observed up to all the principles of influence. It is uncertain how the combination of principles of influence may have affected the results. Such inconsistent conclusions emphasize the requirement for additional research in this domain.

2.7.1 Authority

Authority has always been accepted as a natural requirement and a political necessity. Due to its simple and elementary appeal, authority throughout history served as a model for authoritarian based governments (Arendt, 1958).

Historically, authority was viewed as a simple demand of obedience in pure terms. It was commonly defined as some type of power or violence. It was incompatible with persuasion which assumed equality and worked through a process of argumentation. However, this definition has evolved. It no longer holds such affective true purpose. Instead authority and persuasion have achieved greater correlation and nowadays, authority is considered a principle of influence.

Though it is our human behavior not to query authority, it can be majorly used to source fear. People usually conform to commands to avoid penalties and adverse consequences such as: losing an honor; losing valuable things; embarrassment or criticism.

Authority refers to the inclination towards thoughtlessly agreeing to take the statements and instructions of people and entities who seem to be established on a topic (Milgram, 1974). They simply apply the heuristic regulation: “If an expert says so, it must be true” (Cialdini, 2001). Expert’s position exclusively tends to persuade people (Cialdini, 2001), instead of being convinced by the quality of an authority’s urgings (Sussman et al., 2003). This exercise raises the peripheral (heuristic) cues to persuasion and diminishes the central route (Petty et al., 1986).

Since the authority principle is one persuasion technique (Bullée et al., 2018), it is logical that phishers often use authority as the main practice. Possibly, most individuals do not desire adverse consequences as a result of not agreeing to authoritative figures. Hence, people who obediently respond to authority are more likely to agree and respond to email requests than people who are more doubtful about authoritative figures.

There are two primary kinds of authority:

- Authority based on expertise, such as doctors, police.
- Authority based on the position occupied within a company, like the finance executive of a bank or the manager for a recognized company, for instance, Google, Facebook.

Some studies examined authority in associated situations. For instance, Bullée et al., 2015 conducted a social engineering based study in an experimental in-person situation instead of via email. They found that authority didn’t affect on the susceptibility of users’ towards information revelation. Dressing of the ‘attacker’ was varied to provide different levels of authority, where formal attire represented high authority and casual wear denoted low authority. According to a study conducted by Guéguen et al., 2002, authority indicators in an email signature improved the pact with a simple email request, signifying that authority might be more influential when indicated through a powerful position instead of clothing.

Messages intended to look to come from legitimate authoritative or trustworthy figures such as a company’s employer, bank, health-care authority, may influence receiver to feel obliged to agree to and respond to such requests. Obligation to respond is the trademark of authority. Social learning boosts individuals not to query authority, thereby they are accustomed to reply (Ferreira et al., 2015). On Social Networking Sites, this method may be successful if the invader has formed a striking profile or a page with untrue information planned to make it seem genuine. User’s trust can increase by such fake profile as they may have many followers, updates, photos, mutual friends, building up trustable content and the factors responsible for faith. Otherwise, the invader could imitate a public figure, pretend to be someone victim’s trustable source or create a duplicate a profile (Stajano et al., 2011).

2.7.2 Urgency

From an abstract point of view, despite the growing awareness that decision-making in general is not an entirely rational process, studies in decision making behavior in general have continued to make way for rational decision-making studies. Although advancing our knowledge in certain broader organizational contexts, rational approaches in the email decision-making context need to make way for decisions that are generally bounded by cognition or the limitations of heuristics (Andersson et al., 2014). Recognition of these psychological processes involving urgency and how they are activated may also contribute to a potentially richer understanding of why some email users are prone to phishing attacks. This type of understanding is also crucial for trainers integrating broader considerations into educating email users.

As per the Elaboration Likelihood Model (ELM) (Petty et al., 1986), there are two different approaches according to which people process information: central route and peripheral route. Under the central route (systematic processing), a person’s effort on message’s content and decisions are dependent on skills requiring reasoning. In peripheral processing, a person uses heuristics such as biases, stereotypes, rules of thumb and short-cuts to decrease cognitive burden in decision making (Sunstein et al., 2005). Peripheral processing is more prospective when the decision involves strong affect (emotions), time-limits and cognitive comfort due to trust. For instance, phishing designs can arouse strong emotions by using the scarcity principle. According to the scarcity principle, individuals are driven further by the thought or fear of losing something than by the thought of equal value gains (Cialdini, 2001). Phishing designs can therefore exploit the scarcity principle by warning the customer of future penalties if they do not respond under the ‘official’ time limit. The purpose of this strategy is to scare the person into acting instead of cautiously evaluating the content of the email.

Urgency provides a design aspect to phishing email in order to pressurize the user into a time limit or deadline. As per psychological reactance theory, people focus on things that are scarce and serve their competitive needs (Workman, 2007; Ciadini, 2001).

The first criterion is threat/opportunity: It raises the scarcity principle by providing a rare and quick opportunity for the user to be rewarded for prompt action or a loss or penalty for delayed action. Some users tend to be obedient to the authority considering its uneven power. The scary tactics of penalties leads to a forceful feeling and hence forces users to react hurriedly, out of fear of a possible mistake or summoning as per authoritative orders. Legal jargon such as ‘kindly adhere’ and ‘hereby required’ adds more to these strategies (Workman, 2007; Ciadini, 2001).

Financial reward programs, discounts, and monetary gain provide an aid to entice users by banking firms. For instance, reward programs familiarize customers about the incentive and the need to improve their perceived status. It also provides tangible monetary benefits, and feelings of self-progress. This reward-based mechanism has been greatly exploited by scammers in phishing/spear-phishing.

It is particularly noticeable that urgency indicators can decrease the attention paid to other cues (Vishwanath et al., 2011). Variances in decision information and urgency can impact how vulnerable users are (Vishwanath et al., 2011). A study found that urgency cues (such as time limits or other urgent indications) will reduce attention to other cues and hide the authenticity of the email (Vishwanath et al., 2011).

Timing also serves as an important factor during mimicking transaction(s) that appears to be relevant for the victim at the particular point in time. For example, during tax season tax related phishing email frauds are likely to increase. Email users are the perfect target for social engineering attacks. In terms of email overload, phishing designs rely on a user's tendency to make speedy decisions. Although, specific arguments for the role of urgency and authority cues in email designs are sparse, applying these concepts from social psychology theories jointly may offer new perspective for researchers and fill up the research void. Recognition of these psychological processes and how they are triggered should increase our insights into why some users are more prone to compliance behavior.

2.7.3 Risk Factors and Risk Perception

Finance theory perceives risk in consideration to variance in anticipated returns (Duxbury et al., 2004; Haugen, 1995), while the psychology literature lean towards linking risk to likelihood or proportions of potential losses (e.g. Payne, 1975; Slovic et al., 1968).

While taking risky investment choices, the procedure consists of two steps; risk assessment (perception) and the choice of complying to the risky deal. In a research conducted by Darren et al., 2004, the prime question was whether user's observations regarding investment risk indicate loss aversion or variance aversion. Loss aversion was more supported in results.

Loss aversion can be found in cognitive psychology, decision theory, and behavioral economics. Loss aversion is defined as individual's inclination towards avoiding losses instead of going for equivalent gains: it is preferable not to lose $10 than to discover $10. This principle is prominently used in economics. Loss aversion differs from risk aversion due to individual's utility for a monetary payoff rely on previous experiences or something that was bound to happen based on experience. According to Darren et al., 2004, psychologically, losses are twice as powerful as gains.

Humans have psychologically evolved to be loss averse due to asymmetric evolutionary preference on losses and gains. Loss aversion was first proposed as explanation for the endowment consequence—the fact that individual puts a higher value on a thing that they have than on an identical thing that they don't have (Kahneman et al., 1990).

Given the dominant effect of loss aversion, individuals will look for alteration in down markets (where expected profit is in negative and loss probability is high) since they are better equipped to save themselves by avoiding negative returns. Contrary to this, in profitable markets (loss probability is low and positive returns are possibly high), individuals will attempt to be variance averse and prefer to gain as much profit as they can make. Subsequently, as per Darren et al., 2004, empirical studies measuring and investigating risk should focus on the risk-return trade off relationship distinctly for falling and rising markets.

According to Darren et al., 2004, deliberative risk judgements are favored and supported by most of the experiments conducted for understanding predictability of risk perception. They ignore the effect of experiential based risk decisions. The divisions among affective, deliberative and experiential components of risk are a part of the TRIRISK model. Next, we describe these components in detail.

Deliberative risk perception is defined as a reason-based probability of judgement. It is commonly raised in health based theories and other decision-making based models. *Affective* risk perception refers to feelings that are associated with threats. Feelings can vary as per the valence involved (positive-negative) and the arousal levels (high-low). It is usually measured by anxiety, fear, or worry/feeling of burden based reports. The third category is *experiential* risk perception which involves heuristic risk based judgments taken in response to severity of threat.

As per Alohali et al., 2018, experts perceive and interpret risk on very different notes than non-experts. Though experts use reasoning based on quantitative and qualitative methods, non-experts do not calculate risk in a logical, steady way. They are majorly influenced by perceived damage based causation and often rely on effect of such risk. Furthermore, individual's perception of risk assessments is also based on their ability to think of the outcomes, their personal encounters with such risks (Emma et al., 2018).

Several factors play significant part when influencing individuals on their judgement of perceived risk in information security. Some factors are risk familiarity, variance of fear, anxiety generated by risk, causal effect of such risk, judgement to take risk or not, and severity of the results (Alohali et al., 2018).

Online risks relatable to identifiable risks in physical world are better taken in consideration and are perceived as serious. This concludes that individuals are more mindful of physical losses such as theft and item losses than the online losses such as network based threats, monetary losses through online bank account. This could be attributed to low level of knowledge which can occur due to negligence, low access to such security practices, users' choices to oversee such guidance (Alohali et al., 2018). Also, risk perception has been related to risky behavior in off-line settings. For example, studies found a consistent relationship between health-related risk perceptions and vaccinations (Emma et al., 2018).

While perceived risk for online financial transactions is high when compared to social networking, Davinson et al., 2014 observed low levels of perceived threat for online bank activities, as individuals thought that they are not likely to be target of such frauds. Most interestingly, knowledge and previous experience adds to the prediction of behavioral replies to phishing attacks.

Williams et al., 2018 experimented over the response over phishing emails with authority and urgency cues. Also, they tried finding out other factors that affects such cues in workplace.

Considering the interactions between such factors, we have carried out the collaborative effect of such facts in simulated phishing emails in our research study.

2.8 Framing: Altering Reality

A frame is a psychological device that manipulates salience and offers a perspective in order to influence subsequent judgement.

2.8.1 Message Framing

Message Framing is the art to influence by utilizing information and building communication (Smith et al., 1996). Audiences and individual's response often differ greatly as per the framing of the request. A message may be set up with logic, emotion, ethics and may focus on the incentives of a group or a person.

2.8.2 Using Message Framing for Social Engineering

Words defined within a frame evoke a mental state. Negating the frame is a powerful technique. If someone tells you not to imagine a spider in a web, your brain will automatically picture the spider first and then tell you not to picture it. Telling a target to be cautious about some situations reinforces the desired frame. This technique is often used by professional social engineers. Framing is effective as it keeps the truth and bends it so that it remains believable, but not so much that it becomes false.

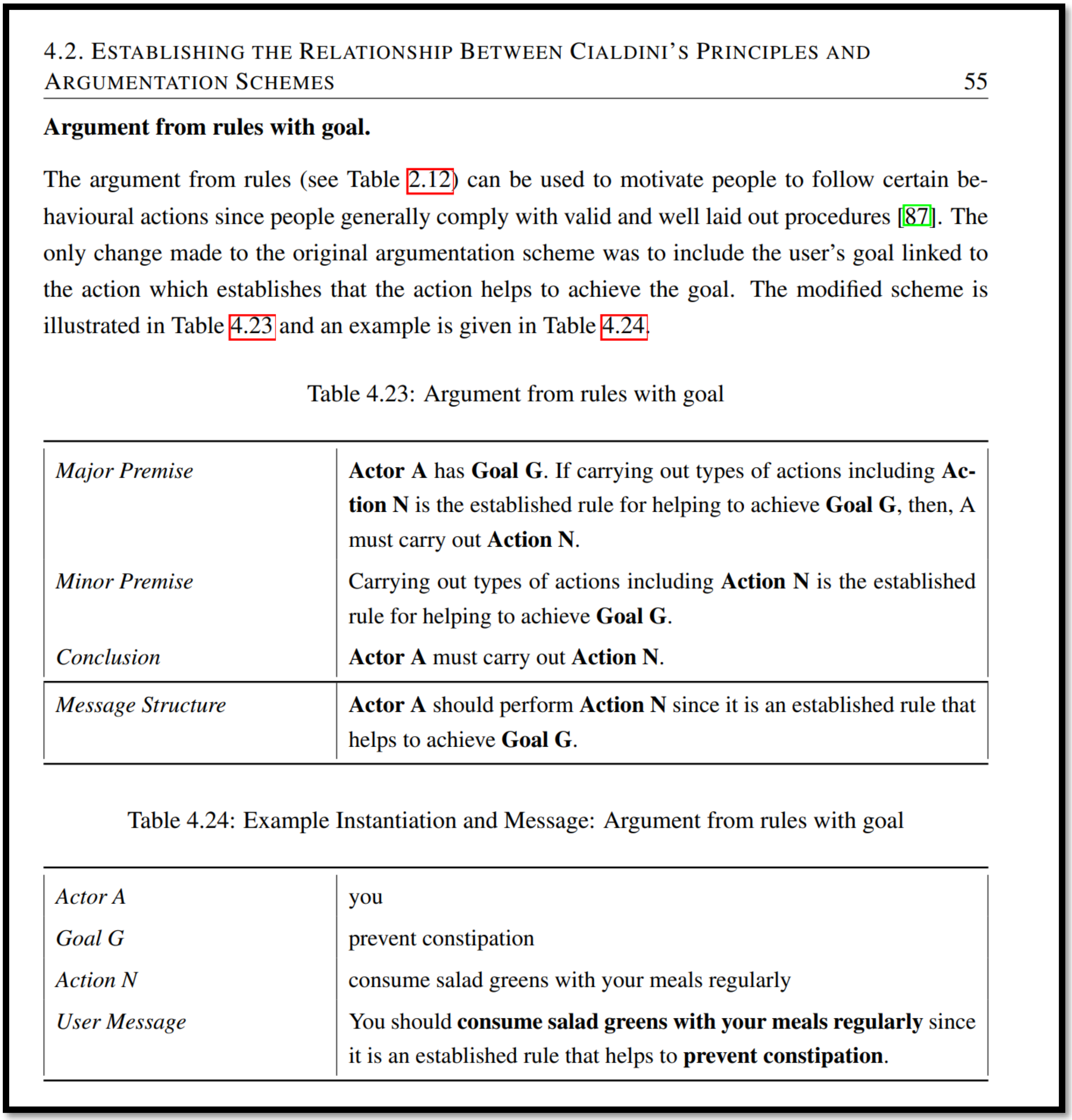
To professionally frame questions used in the study to have the supreme result, following principles can be followed ("Framing" (n.d.)):

- Each question should be phrased so that it has one and only one clear purpose
- Technical jargons that confuse the individual or weakens the cause should be avoided
- Questions should be framed to focus on individual's behavioral type (amiable, critical, expressive)
- Focus on the purpose of the question and what information we require by asking it to the individual

2.8.3 Argumentation scheme

Argumentation schemes are stereotypical patterns of reasoning or arguments from premises to conclusion that make-up common kinds of assumptions used in day-to-day communications and in specific contexts (e.g., judicial, scientific) (Walton et al., 2008). Argumentation schemes are comprised of deductive and inductive types of arguments. Under deductive argument, the purpose of the premise is to provide strong support for the conclusion so that, if the premise is true, then it would be infeasible for the conclusion to be false. In an inductive argument, the premise aims to be sufficiently strong so that, if the premise is true, then it would not be likely that the conclusion is false. This is frequently used in artificial intelligence (Walton et al., 2002).

Argument from rules with goal provides motivation to people to follow certain behavioral actions since people generally comply with valid and well laid out procedures. In our study, we use argument from rules with goal which supports authority and urgency principles of influence (Josekutty, 2019).



4.2. ESTABLISHING THE RELATIONSHIP BETWEEN CIALDINI'S PRINCIPLES AND ARGUMENTATION SCHEMES 55

Argument from rules with goal.

The argument from rules (see Table 2.12) can be used to motivate people to follow certain behavioural actions since people generally comply with valid and well laid out procedures [87]. The only change made to the original argumentation scheme was to include the user's goal linked to the action which establishes that the action helps to achieve the goal. The modified scheme is illustrated in Table 4.23 and an example is given in Table 4.24.

Table 4.23: Argument from rules with goal

Major Premise	**Actor A** has **Goal G**. If carrying out types of actions including **Action N** is the established rule for helping to achieve **Goal G**, then, A must carry out **Action N**.
Minor Premise	Carrying out types of actions including **Action N** is the established rule for helping to achieve **Goal G**.
Conclusion	**Actor A** must carry out **Action N**.
Message Structure	**Actor A** should perform **Action N** since it is an established rule that helps to achieve **Goal G**.

Table 4.24: Example Instantiation and Message: Argument from rules with goal

Actor A	you
Goal G	prevent constipation
Action N	consume salad greens with your meals regularly
User Message	You should **consume salad greens with your meals regularly** since it is an established rule that helps to **prevent constipation**.

Figure 2. Argumentation Schemes (Josekutty, 2019)

2.9 Personality traits

The Big Five personality dimensions, also known by OCEAN model, is a nomenclature for personality traits. Multiple facets of the personality traits can be used to describe the person and clarify ambiguities.

The big five factors are:

- **O**penness to experience: general appreciation for experience (consistent/cautious vs. inventive/curious)
- **C**onscientiousness: people control, regulate, and direct their impulses (easy-going/careless vs. efficient/organized)
- **E**xtraversion: engagement with the external world (solitary/reserved vs. outgoing/energetic)
- **A**greeableness: individual differences in social harmony (challenging/detached vs. friendly/compassionate)
- **N**euroticism: tendency to experience negative emotions i.e. anxiety, nervous (secure/confident vs. sensitive/nervous)

Each factor is a product of correlated and more specific primary factors e.g. extraversion includes gregariousness, excitement seeking, warmth, positive emotions and assertiveness.

2.9.1 Personality and persuasion

Some people tend to be constantly highly amenable to social influence whereas others are greatly resistant (Janis et al., 1954). Personality provides various implementation of persuasion models. When considering authoritarianism, it moderates the impact of persuasive messages highlighting reward vs. threat. When considering argument quality, high authoritarians perceive threat message as stronger compared to reward based message. However, low authoritarians perceive the reward message as solid when compared to the threat message (Lavine et al., 1999).

2.9.2 Personality and social engineering

Nowadays, behavioral derivation from personality traits holds a great potential research (Simkins et al., 2010). Until now, personality assessment focused on the relations between social media and other digital records with conventional personality measures (Bleidorn et al., 2019). Detection of persuasive textual arguments through personality traits of author and victim with their interaction is becoming a common phenomenon. When considering parties' personality traits, focusing on features that seize on author-reader personality traits and their collaboration can increase the efficiency in detecting persuasive arguments (Shmueli-Scheuer et al., 2019).

Decision based actions under risk is assumed to be formed out of pure logic under classical decision theory. Under such assumptions, reasonable people tend to make rational picks on the basis of unbiased factors.

Persuader tries to influence persuade with some incentives and specific goal (e.g. altering one's attitude towards a specific issue). Success of a persuasive work depends on the quality of the message/argument, and more importantly, to the personality of the persuadee (Jacob et al., 2012), the nature of the persuader (Anthony et al., 2016). Association among personalities of both groups and the influence of the argument as projected by its textual characteristics serves the purpose of understanding influence in the argument.

2.9.3 The social engineering personality framework

People with high ethics in extraversion are driven by rewards and social consideration, based on their motivations (Ashton et al., 2002). Communal goals and interpersonal harmony correspond to high values in agreeableness. Conscientious people are inspired via order, achievement and proficiency. Individuals with high values in openness are greatly subtle to creativity, innovation, and intellectual stimulation, whereas neuroticism corresponds with threats and uncertainty (Hirsh et al., 2012). Three personality traits - extraversion, conscientiousness, and openness demonstrate both increased and reduced users' susceptibility to social engineering. Agreeableness upsurges and neuroticism declines susceptibility rate (Uebelacker et al., 2014).

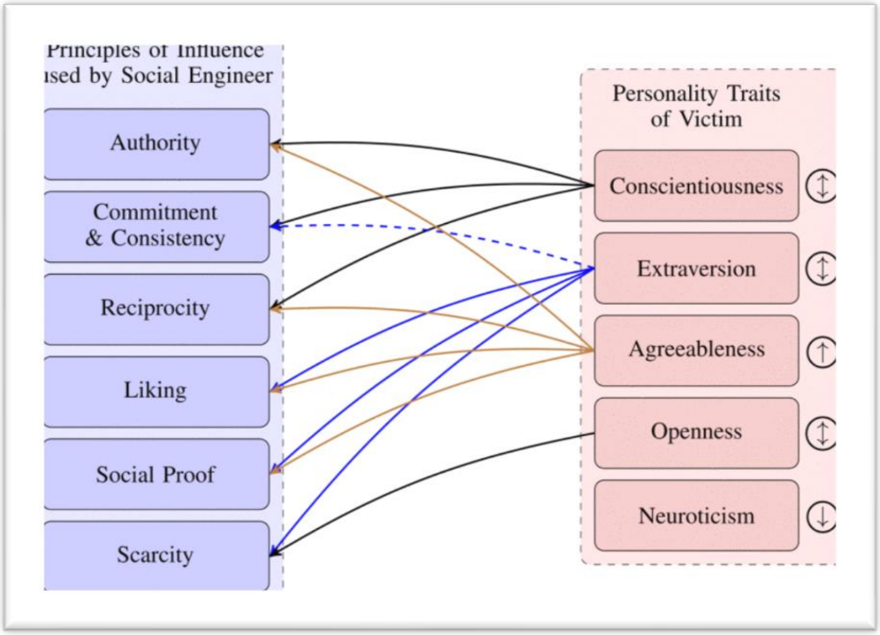


Figure 3. Social Engineering Personality Framework

As per Big Five model, specific personality traits of a target increases (solid line) or reduces (dashed line) the susceptibility to Cialdini's influence principles. Overall personality norms about susceptibility (higher, lower, or both) for each attribute are represented by corresponding arrows (↑,↓,↕). (Uebelacker et al., 2014)

According to Uebelacker et al., 2014, Social Engineering Personality Framework (SEPF) framework explains variances in vulnerability to Social Engineering and will lead researchers by giving a structured method. Thus, adapting mitigation approaches as per every personality and level of variation can be beneficial. Detecting Social Engineering attacks via flow charts, penetration tests, questionnaires by considering which links alter the susceptibility to Social Engineering attacks or by predicting the categories of attacks which are more probable to thrive in a specific employee's pattern.

In our study, we seek to understand the collaborative relation between authority, urgency, experience, risk perception, human factors, personality traits (as mentioned in social engineering personality framework) and user's susceptibility to phishing emails.

2.10 Phishing and spear-phishing

With rising figure of threats and stricter business guidelines, organizations are constantly tested in security and compliance in IT organizations. While scams and deceits are readily common, the rapidness and range has increased extremely with the world's growing necessity over the Internet, email and social media platforms. To quote, the spread of usage of email inside the organizations have not only smoothed the success of businesses, it has also unlocked a door to significant security threats.

Spear-phishing efforts are made even simpler with the wide information availability on social and other platforms being placed on the Internet openly. With social networking sites popularity rising up, users are increasingly trusting such platforms with large volumes of private and sensitive information, such as their current living place, their occupation, date of birth and interests. Such information can easily be gathered by cyber-criminals without any technical expertise and with very little struggle. Status updates willingly provide hackers with all the necessary information they need to create an email that is personal and relatable by the targeted victim (Bimal et al., 2012).

With the wider reach of internet across domains, minute information is also available or can be derived accordingly. This possess a threat for users sharing their information. Spear-phishing is becoming more effective as it is primarily tough for users to differentiate genuine emails from spear-phishing emails without additional defensive mechanisms (Duman et al., 2016).

2.10.1 Personality type and internet behavior

In the cyber-security field, researchers have started to give more emphasis on role of different aspects of psychology that can be used to gain access to internet security. One existing point of concern is that normal social activities may be replaced by the internet and that individuals who are obsessed with internet may be compensating for social seclusion and loneliness.

Schrammel et al., 2009 conducted a study and found no correlation among personality traits and information disclosure online, instead found correlation among information disclosure and time spent in online internet activities.

2.10.2 Internet usage and risky activities

Optimistic bias is predominant in the literature since it connects to many off-line risks and activities. Campbell et. al., 2007, focused on users' estimation of likelihood to engage in positive internet activities vs. risky online activities. The study found that the student participants favored their online activities, with heavy internet users reporting a higher optimistic bias than light internet users.

2.10.3 Phishing vulnerability, judgment error and trust

Replying to phishing outcomes from an error of decision just like when responding to scams. Understanding psychological traits that root certain individuals to perform such errors is of prime importance in research. Finding gaps of judgement in online activities (such as updating sensitive personal information on social networks websites) has been explored by Halevi et al., 2015. The success or failure of a phishing attack relies on individuals answering to it and revealing their information. Hence, considering the psychological motives for replying to such emails is imperative to creating effective defense mechanisms to avoid such phishing attacks.

Exploitation of user trust is the ultimate goal of phishing. People tend to trust and cooperate with other people due to evolutionary reasons (Hill et al., 2006). Users 'trust' of online parties is a dependent factor in making online transactions. Still, internet users often make wrong 'trust-based' decisions. Awareness of phishing and other cyber-attacks may elevate the user distrust of online entities. Kumaraguru et. al., 2006 established a trust model for online activities, that distinguished between 'experts' and 'non-experts'. The study showed that online 'experts', who have a high level of familiarity with internet threats and defenses, are more likely to detect correctly signals of a suspicious email and distrust it vs. 'non-experts' users, who are less familiar with the signals of malicious emails.

2.10.4 Financial sector and phishing

Since the initiation of the Internet, human reliance on digital platforms and communicational technologies and other networked technologies for jobs ranging from everyday simple information-based web surfing to more noteworthy and serious tasks, such as financial transactions and manufacturing, precise operation, has steadily increased.

This reliance has converted into a rising importance on the planned standing of cyberspace to enable accomplishing essential objectives in modern societies: invention, competition, partnership, efficiency and guidance.

While establishments and individuals are taking advantage of its business profits, they fail to comprehend that cyberspace offers the same assistances to those who focus on attacking them. Hacker associations, criminal groups worldwide have admission to powerful, evolving competences, that are used to recognize, target and attack the internet users. These attacks also consists of behavioral, psychological threats apart from technological threats. If we accept the point that contemporary, economically advanced societies are progressively converting as 'information societies', then, it can be directly seen that such threats to data and related information can be seen as problems that can affect the core of these societies (Eriksson et al., 2006).

While everyone agrees with the need of shielding cyberspace from criminal activities, our thoughtfulness about cyber-crime and its related penalties, both socially and economically, is still incomplete. Due to wide differences in viewpoints and a lack of agreement on numerous essential topics of cyber-crime, the literature on cyber-crime is still low and weak. Furthermore, the intangible pre-conditions such as perceptions of risks, trusts, general fears, feelings of insecurity have significant consequences (Monica et al., 2014 and Maheshwari, 2011).

Adopting broader approach, following can be regarded as cyber-crime (Monica et al., 2014 and Maheshwari, 2011):

(1) *Traditional crimes*– crimes that are conducted online and exploits cyberspace by giving more gaps and loopholes (e.g. traditional fraud, piracy, surveillance, stalking)

(2) *Hybrid cyber-crimes*– old-style crimes whose accomplishment, boundaries have meaningfully transformed as an outcome of new prospects created by the Internet (e.g., information theft, hacking).

(3) *True cyber-crimes*– includes chances formed completely by the Internet and performed only inside cyberspace (for instance denial of service, phishing attacks, spamming) (Wall, 2003).

(4) *Cyber platform crimes* such as botnet usage to facilitate crimes remotely without knowledge of users and facilitating the exploiting of users indirectly.

Driving into the digital banking sector, cost-effective and fast customer service access provides an inbound advantage of using internet banking as a platform. The clerical labor gets reduced considerably with Internet banking facilities. Expenses on bank writing materials have lowered, thereby raising the turnover of the bank by a huge figure. Customers gain the advantage of available account information anytime, regardless of their physical location. Online banking becomes less safe and secure if users are not much aware of cyber-crime or less aware of using such digital platforms. A progressively widespread criminal exercise is to gain access to an individual's finances is phishing, by which the user is influenced and convinced by several means to hand over their sensitive information to a fraudster. Financial sector phishing scams are not only limited to digital platforms. Instead scam calls, spear-phishing are also increasing these days as they tend to exploit new versions of human knowledge limitations in technical domain (Monica et al., 2014 and Maheshwari, 2011).

2.11 Limitations with phishing research

The hierarchical nature of workplaces or government organizations makes users more susceptible towards authority and urgency methods (Stajano et al., 2011). There is considerable amount to be determined by exploring the role of such factors and influence practices.

Primary aspects that may influence users’ susceptibility to phishing emails have been researched over the last decade. There has been development of a variety of theoretical frameworks, such as Protection Motivation Theory (PMT; Rogers, 1975), Integrated Information Processing Model of

Phishing Susceptibility (IIPM; Vishwanath et al., 2011) and the Suspicion, Cognition, and Automaticity Model (SCAM; Vishwanath et al., 2018).

While most of these models show a degree of overlay, the factors mentioned in these models have hardly been studied together. For instance, the SCAM model combines user's knowledge, views and behaviors in relation to susceptibility towards phishing emails. PMT has been more generally used in common security behavior and scrutinizes user's threat perception levels and perceived aptitude to deal with such attacks. Lastly, the IIPM focuses majorly on the information processing way by the users when presented with a phishing email. These models have not been studied using a structured hierarchical based dataset with all the overlapping factors in effect. Exploring these parts within such settings can provide a sole chance to comprehend all factors that may influence users' susceptibility in such hierarchical atmosphere.

Authority cues focus on impersonating organizations or individuals that are esteemed and have a degree of authority by the recipient. Urgency cues include putting people under a situation with a degree of time pressure that pushes them to respond speedily. While individual's approach to risk has been recommended to vary as per a specific situation and field (i.e., financial vs. health organization) (Weber et al., 2002; Ermer et al., 2008), personality traits such as short self-control, adventurous and thrill-seeking have all been related with risky actions across various areas (Mishra, 2014). Broader factors have also been revealed to impact risk-taking behavior, such as volatile or disruptive social surroundings (Mishra et al., 2008). Earlier work has shown that the existence of authority and urgency cues in phishing emails can increase the susceptibility in other situations (Parsons et al., 2019) and in offices (Williams et al., 2018)

To conclude, risk perception, urgency, principles of influence and personality traits have been explored in pairs, the serial affect has not been analyzed. Framed phishing emails in terms of authority-based persuasion principle for social engineering has not been analyzed when considering contextual factors, personality traits of victims, urgency and risk factors.

CHAPTER 3. METHODS

This study investigates the gap of possible associations between principle of influences (authority, urgency) and various user contextual, behavioral factors. The key purpose of this research is to examine whether the presence of urgency, authority cues, human factors for certain personality traits differentially impact the users' susceptibility to phishing emails. Secondly, check whether presence of risk factor along with varying degree of authority, urgency cues impact the user's susceptibility. This chapter outlines the research paradigm, approach, and design that were used to achieve the purposes of the research study.

3.1 Research Details

The study seeks to answer following research questions:

RQ1. Does presence of authority and cues within phishing emails affects the likelihood of responding to phishing emails?

RQ2. Does presence of risk perception affect the likelihood of responding to phishing emails?

RQ3. Does falling victim to phishing emails previously affect the likelihood of responding to phishing emails?

RQ4. Do personality traits affect the principles of influence when responding to phishing emails?

3.2 Research Design

In this research, we performed a survey of authority, urgency, risk perception and human factors involved in phishing and a study to associate conditional probabilities of such factors in phishing emails. The association will be verified using a survey which is a tool for determining behaviors and intentions of people/populations. Survey research is one of the key areas in applied social research field. In this study, we will design web-based questionnaire as the method of survey since it's very cost-effective and convenient. In a web-based survey, questionnaire can be circulated via the web link and the participant’s opinions/scores of particular items could be automatically collected and recorded into the database.

The aim of this study is to investigate the relationship between dependent variables (susceptibility to phishing emails) and independent variables (contextual and human factors). These relationships were tested using survey instruments.

In developing and designing our experiment, we framed phishing emails with varying degree of authority, urgency cues first and risk cues. We compiled the templates in financial field and tactics used by phishers in emails. The first set of questions consists of varying degree of authority, urgency cues. Then, next set of questions consists of varying degree of authority, urgency, risk cues.

3.3 Survey implementation and instrument’s validity, reliability

For the implementation of the survey, we will be using reliable survey instruments.

3.3.1 Survey Questionnaire

The questionnaire/survey included the following:

Demographics:
Gender, age group and ethnicity-based questions

Risk-taking:

We used IPIP-scale based risk-taking personality questions in this survey. For the 20-item IPIP scale, all alpha coefficients ranged in between .87 to .93 (Zheng et al., 2008). For the short 10-item versions, the Agreeableness reliability was lower (.69 and .66, respectively), whereas all others were substantial (ranging from .76 to .87) (Zheng et al., 2008).

Big Five Inventory:

Five personality domains (conscientiousness, agreeableness , extraversion, openness, and neuroticism) have been constantly recognized using various instruments and across many beliefs and is therefore a highly looked upon classification. The Big Five Inventory scale used for this research area is a self-described 44-item questionnaire to which participants are questioned to indicate over 5-Likert scale whether they strongly disagree, disagree, are neutral, agree, or strongly agree. Higher scores within the personality domains indicate a greater tendency for the personality trait being calculated. This personality inventory has been widely used, demonstrating good validity and reliability (McCrae et al., 1999). This scale shows substantial internal consistency, retest reliability, and clear factor structure, as well as considerable convergent and discriminant validity with longer Big Five measures (Benet-Martínez et al., 1998; John et al., 2010).

Internet usage:

A 5-questions short survey adapted from Campbell et al., 2006 and Young et al., 2011 will be used. These studies showed Cronchbach alpha to be above 0.70 for each factor in consideration. The survey asked the users about their online distinctive behavior, including what activities they perform online.

Fallen for phishing:

Question set describing if a person has fallen for phishing or not. If yes, another set of questions were asked detailing about the types of losses.

Set of phishing emails with varying degrees of urgency, authority, risk cues:

This consists of two sets of phishing emails in financial domain. In first, variation of authority, urgency was used to serve as cues to frame phishing emails. In the second set, varying degree of authority, urgency and risk were used as cues to frame phishing emails.

3.4 Variables

The study defines one dependent variable of click-rate. The study organizes the emails into varying degrees of authority, risk, urgency factors. The first email set contain varying degree of authority and urgency components. The second set has authority, risk, urgency in varying degree of component in the emails. Grouping these emails into two different types lessens the data to be more controllable for testing. The emails are principally casted to focus in financial domain.

In both sets, we are measuring the respective effects on click-rate, which is defined as the share of users who click on malicious links within the email and find them legitimate. Click-rate has been measured using Likert scale.

To calculate the susceptibility to phishing emails of users, the study analyzes the dependent variables (users' susceptibility to phishing email) related to contextual and human factors of the users. The following variables contribute to contextual and human factors of the users which are measured in the survey for every user –

- **Internet Time** – measures how many hours a user spends online in an average week,
- **Ethnicity** – records the type of ethnicity a user belongs to,
- **FallenPhishingVictim** – records whether a user has fallen victim to phishing emails or not. If yes, it asks about the consequences of the event by checking all that applies,
- **Gender** – records the gender of the user,
- **Age** – records the age group under which users age falls,
- **RiskAttitude** – measures whether a person prefers taking risky decisions,
- **Personality traits** – measures 'Extraversion', 'Agreeableness', 'Conscientiousness', 'Neuroticism', 'Openness' personality traits which comes under BFI personality scale.

3.5 Creating Phishing Emails

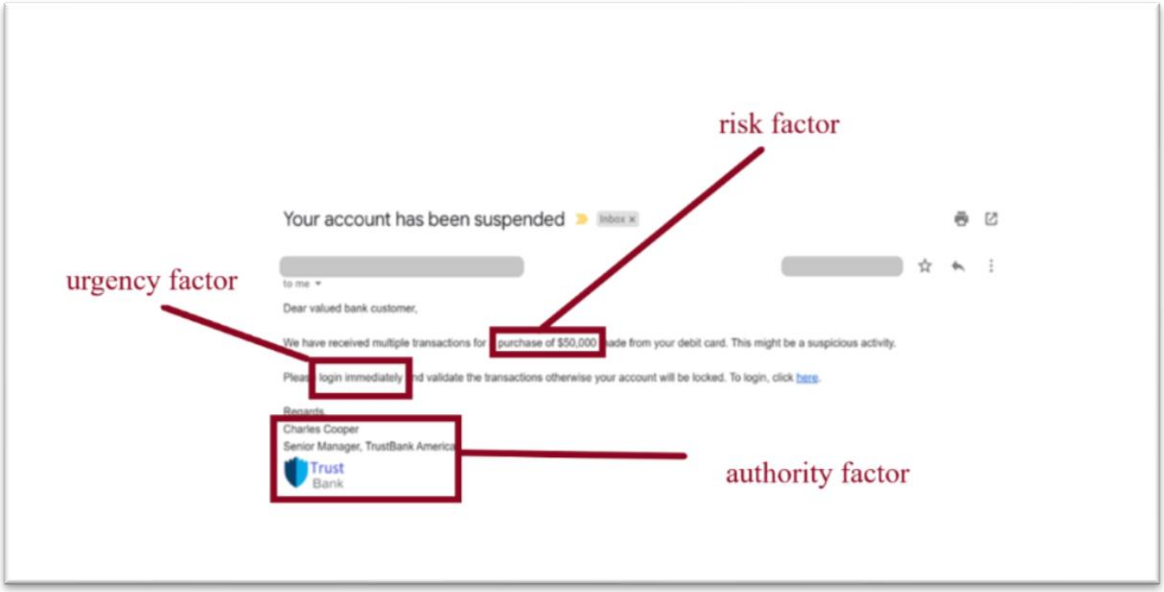
For each phishing email, subject and content were discretely curated. For this study, each 29-phishing emails was independently created to display email features that might indicate a phishing attempt. Attention was paid to presentation and body composition.

The first distinguished presentation factor is anonymous greetings and attitude of the emails. Once initiated, an email should persist to keep the target's attention by sounding legitimate. Also, the receiver observes how the opening and closing lines of the email are composed.

Hyperlinks are the supreme technique used by social engineers to try to break into systems. When clicked, a hyperlink could perform various functions as per the tailored needs such as directing user to a fraudulent site to enter sensitive information that can be collected by social engineers or downloading malicious content on users' system. We used embedded hyperlinks in all of our study's phishing emails.

As seen in Figure 4 below, we added urgency, authority, risk factors in the email with anonymous greeting as well as a malicious hyperlink. As seen in the Figure, we added a risk factor as reciprocated on the basis of money. Adding urgency gives a sense of appeal to the phishing emails which blurs down other nuances to be caught as phishing emails. Authority gives a legitimate perspective to the emails. Here, we can see the authority in the emails as of high level, which provides cues to be perceived as legitimate.

To aid fake emails appear legitimate, social engineers use logos and we added them in our curated phishing emails. An implicit level of trust fills up in the recipient when using a company logo that a recipient will recognize. Such trust levels possessed by the recipient for legitimate company will make them more susceptible to click on links with the intention of doing their portion in helping the company with the demand, which displays the central ideas of Social Exchange Theory (Emerson et al., 1976). Social engineers can use the precise image of the logo of a company putting recipients in a position where they cannot differentiate between legitimate and malicious emails. Despite having an official logo in the email, recipient should critically scrutinize the rest of the email for phishing related email cues indicating the authenticity of the email.



Your account has been suspended

[redacted] [redacted]

to me

Dear valued bank customer,

We have received multiple transactions for purchase of $50,000 ade from your debit card. This might be a suspicious activity.

Pleas login immediately nd validate the transactions otherwise your account will be locked. To login, click here.

Regards

Charles Cooper

Senior Manager, TrustBank America

Trust
Bank

Figure 4. Illustration showing structuring of an email with the cues

CHAPTER 4. RESULTS AND DISCUSSIONS

We conducted data collection over Amazon MTurk after an approved IRB application at Purdue University (IRB-2020-819). Respondents were 18 years or above. We received 379 responses with 244 males and 115 female participants. Ethnicity-wise distribution shows 278 were White, 52 were Black or African American, 7 were American Indian or Alaska Native, 17 were Asian, 1 was Native Hawaiian or Pacific Islander and 5 were of ‘other’ ethnicity. The participants ranged in age from 18 to over 70 with the majority of the participants falling into the 25-29 (27%) and 30-34 (23%) age groups. Only those participants are included in the analysis who successfully completed the survey used in our research. The final sample comprised of 352 participants.

This chapter presents the quantitative data analysis methods used in this study and explains the descriptive results of the survey. It examines and explicates the outcomes of the overall research.

To analyze the data from survey, we used SPSS software version 26. We further present the resuls of this analysis in detail.

4.1 Data Preparation

Data preparation serves a vital step formulate data ready for analysis purpose. We prepared the data for analysis by following the four steps as suggested by Fink, 2015: data coding, data entry, data cleaning, and finding missing values. These steps are explained below:

1. Data coding: Construct a code book for data and the features. For example, the high risk, medium risk and low risk were coded as ‘riskhigh’, ‘riskmedium’, ‘risklow’ respectively.
2. The data was collected online and hence it were recorded electronically. Also, dataset had to be cleaned up of unconnected, irrelevant entries.
3. Data eligibility: In this step, data is examined for possible ineligibility. It consists of two phases: data eligibility and response eligibility. For example, for scale-based questions, data should be between 1 to 5. Response eligibility comprises of keeping a check on the answers such that they are not closely identical for all questions.

4. Missing values: For participants who left the survey in between and did not submit answers to the required questions, we considered their data as incomplete and omitted their record from the dataset.
5. We first entered the survey data into a Microsoft Excel file and then exported it to SPSS software.

4.2 Descriptive Outcomes

In this section, we summarize the descriptive data, starting with the demographic items collected in the study.

4.2.1 Demographic items

There was variance in the demographic items in the study, as explained below.

4.2.1.1 Age, gender and ethnicity

In the study, 68.3% of the 352 participants were male and 30.6% were female. About 76.4% of the participants were white, 14.3% were black or African American, 4.8% were Asian, 0.3% were Native Hawaiian or Pacific Islander and 1.7% were others. About 27% of the participants were 25-29 years old, 23% belonged to 30-34 age group, 12.9% were in between 34-39 years in age. 8.4% and 8.1% of the participants were of 40-44 years and 45-49 years age group respectively. Remaining were greater older than 50 years.

4.2.1.2 Internet Usage and activities

Participants from the study were asked about their usage of internet, specifically how much time they spent online for work, leisure, and other activities. 63 participants reported 40 hours of work every week online, 23 participants reported 30 hours of work per week online, 24 participants mentioned 20 hours of work per week online (Figure 6).

For leisure purpose – 50 participants reported 10 hours per week, 44 chose 2 hours per week, 35 selected 5 hours per week, 34 said 20 hours per week, 25 selected 4 hours per week, 23 said 1 hour per week. Distribution can be seen in Figure 7. 92 participants reported 0 hours per week, 39 said

5 hours per week, other batch of 39 selected 1 hour every week, 32 of total participants said 2 hours/week. Distribution can be seen in Figure 8.

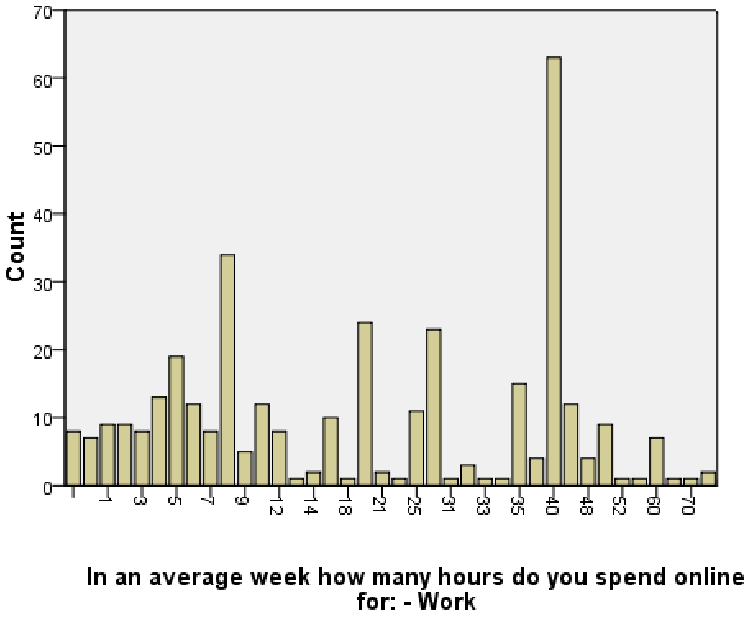


Figure 5. Distribution of users with weekly work hours

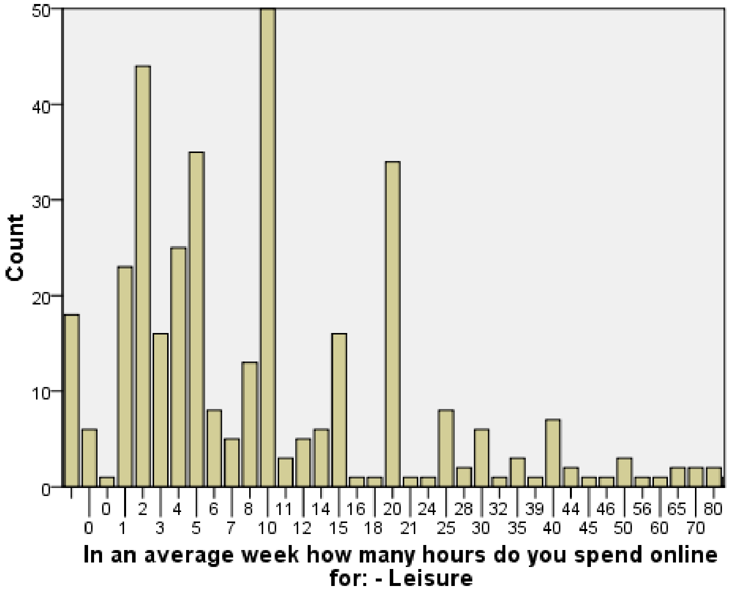


Figure 6. Distribution of users with weekly leisure hours

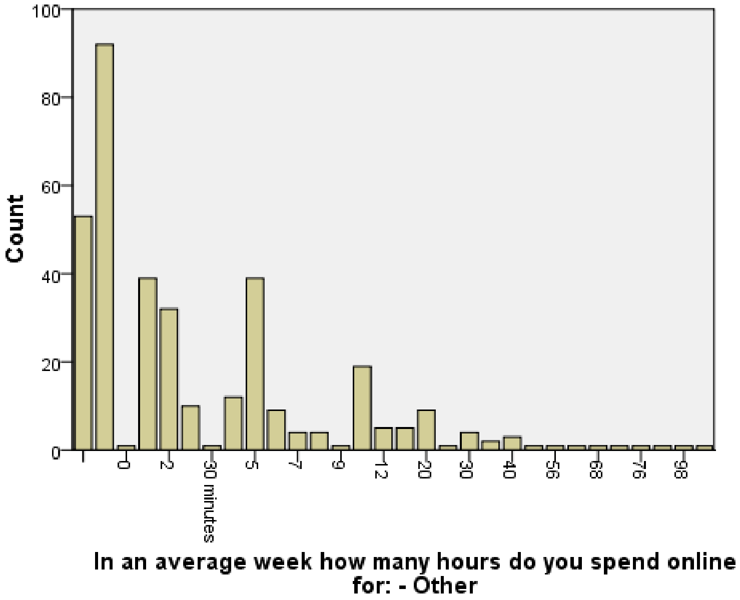


Figure 7. Distribution of users with weekly other hours

4.2.1.3 Risk taking personality

Participants were questioned to rate five items associated to risk taking personality, using a 5-point Likert scale. About half of the respondents reported being low risk takers (M = 2.52, Table 1).

4.2.1.4 Big Five personality dimensions

In the study, participants were questioned to rate themselves using a 5-point Likert scale (Strongly disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Strongly agree) in terms of Big Five Inventory (BFI): a 44-item inventory computing an individual’s personality dimension using Big Five Factors (Goldberg, 1993). These factors are then classified into personality characters – Conscientiousness, Neuroticism, Extraversion, Agreeableness, Openness. As mentioned in Table 1, respondents were more possible to be of extraversion, agreeableness, conscientiousness, openness personality type.

Table 1. Descriptive statistics of personality

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
RISK	338	1.00	4.60	2.5249	.77813
EXTRAVERSION	333	1.00	5.00	3.0413	.68903
AGREEABLENESS	327	1.44	5.00	3.5090	.70013
CONSC	337	1.78	5.00	3.5849	.72221
NEURO	337	1.00	5.00	2.8650	.85947
OPEN	335	1.40	4.90	3.6266	.58009
Valid N (listwise)	292				

4.2.1.5 Previous Phishing Victimization

In this study, about 57% of the respondents reported that they have not fallen a victim to phishing email(s). 33% responded being a victim of a phishing email. We further asked them about the consequences of being a victim. 13 % reported having lost a little money, defined as less than $500. 8.5% reported having lost a great deal of money, defined as more than $500. 11%reported having to change their log in credentials. 12.4% reported losing control of one or more of their accounts. 10% reported being the victims of identity theft. 6% reported that the company they worked for was negatively impacted as a result of their falling victim to a phishing email. 8% reported their computer being infected with a virus as a result of a phishing email. 4.5% reported being a victim of ransomware as a result of a phishing email. 3% reported no consequences.

4.3 Hypothesis Testing

This section elaborates the results attained from hypothesis testing. We worked on our hypothesis and tested them. Multiple statistical techniques were used to test and examine our proposed hypotheses. We used paired sample t-Test, correlation, Levene's test for equality of variances for data analysis.

4.3.1 Testing the relationship between principles of influence and personality traits

- **Testing the relationship between personality traits and authority**

  As per the social engineering personality framework, we devised the hypothesis H1. Testing the correlation between personality traits and authority, we found that authority is positively correlated to conscientiousness *r(333)=.414, p<.00* and agreeableness *r(323) = .345, p<.00*.

- **Testing the relationship between Personality traits and urgency**

  As per the social engineering personality framework, we devised the hypothesis H2. We found that urgency is positively correlated to extraversion *r(331) = .245, p<.00* but there was no significant correlation with openness.

4.3.2 Relationship between fallen for phishing and principles of influence and risk

- **Testing the relationship between falling for phishing and authority**

  For hypothesis H3, we conducted descriptive statistics and Levene's test for equality of variance. We found significance difference *t(312) = 9.04, p<.00* for those who have fallen for phishing (M = 3.40, SD= 1.25) as opposed to those who had not (M = 2.35, SD =1.41) and had significant correlation with authority as principle of influence. Hence, H3 – People who were victims of phishing are more likely to be influenced by authority is supported.

- **Testing the relationship between Fallen for phishing and urgency**

  For hypothesis H4, we conducted descriptive statistics and Levene's test for equality of variance. We found significance level *t(314) = 9.09, p<.00* for those who have fallen for phishing (M=3.75, SD = 1.2) than those who had not (M=2.28, SD = 1.5) and had significant correlation with urgency. Hence, H4 – People who were victims of phishing are more likely to be influenced by urgency is supported.

- **Testing the relationship between Fallen for phishing and influence by risk**

  For hypothesis H5, we conducted descriptive statistics and Levene's test for equality of variance. We found significance *t(306) = 8.606, p<.00* for those who have fallen for phishing (M = 3.63, SD =1.27) as opposed to those who had not (M=2.35, SD = 1.4) and had significant correlation with risk. Hence, H5 – People who were victims of phishing are more likely to be influenced by risk is supported.

4.3.3 Users' susceptibility as a consequence

Our study's major hypothesis is that predictor variables – authority, risk and urgency, have an influence on users' susceptibility towards phishing email (i.e. possibility that she/he would answer to a phishing email). Following are the hypothesis and their respective results –

- **Relationship between authoritative emails and users' susceptibility to clicking phishing emails**
  To find relationship between authoritative emails and users' susceptibility, we checked pairwise sample t Test. We found that authoritative emails are more likely to result in users' susceptibility to phishing emails (Hypothesis H6). The click rate for high authority (M=3.16, SD = 1.4) was significantly different from the click rate for low authority (M=2.83, SD = 1.4); *t(338) = -5.17, p<.000.*

- **Testing the relationship between emails containing urgency language and users' susceptibility to phishing emails**
  To find relationship between urgency language and users' susceptibility, we checked pairwise sample t Test. We found that emails containing urgency language are more likely to result in users' susceptibility to phishing emails (Hypothesis H7). The click rate for high urgency (M=2.74, SD = 1.5) was not significantly different from the click rate for low urgency (M=2.83, SD = 1.4); *t(334) = -2.07, p=.21.*

- **Testing the relationship between risk perception and users' susceptibility to phishing email**
  To find relationship between risk perception language and users' susceptibility, we checked pairwise sample t Test. We found that emails containing risk perception are less likely to result in users' susceptibility to phishing emails (opposite of Hypothesis H8). The

click rate for high risk (M=2.75, SD = 1.4) was significantly not different from the click rate for low risk (M=2.68, SD = 1.4); *t(334) = 1.25, p = .21.*

- **Testing the relationship between authority and urgency interact affecting users' susceptibility**

  Looking at the descriptive statistics of authority and urgency variables of different variance the majority of the user favored low authority – high urgency susceptibility.

  In our research study, authority and urgency interaction supports users' susceptibility weakly. Paired sample t- test was performed for low authority – low urgency, low authority – high urgency variables. The results weakly support hypothesis H9. The click rate for low authority-low urgency (M=2.93, SD = 1.4) was significantly different from the click rate for low urgency – high authority (M=3.04, SD = 1.4); *t(334) = -1.98, p = .04*

- **Testing the relationship between authority, risk and urgency interact affecting users' susceptibility**

  Another major hypothesis H10 is that predictor variables – authority, risk and urgency, have an impact on users' susceptibility. Looking at the descriptive statistics of authority and urgency variables of different variance, majority of the user favored low authority – high urgency susceptibility. Authority, risk and urgency interaction didn't support users' susceptibility.

4.3.4 Discussion

Our results confirm that users' susceptibility is affected by authority, urgency, and risk perception (in various combinations). Perceived email richness, depicting user characteristic, affects users' susceptibility thereby surges the number of cues users can rely on to identify the legitimacy of an email. Phishing email cues serves as activators for detection. Such cues require attention for identification of specific features which may go unnoticed by ordinary users.

Users' susceptibility gets enhanced by two features— urgency and authority. Culprits of a phishing attack can exploit these characters. Trustworthy authorities serve as the phishing email cues and aid in providing credible factors to phishing emails. Users with high levels of submissiveness are less likely to question the legitimacy of emails that pretend to come from a trustworthy entity.

Users' susceptibility is increased by high submissiveness. Users inclined to be highly submissive are more likely to obey orders which eventually decreases their questioning ability in a phishing email.

Users with certain types of personality traits can be majorly influenced by the criminals of a phishing email attack. Authoritative emails majorly affect users with personality traits as conscientiousness and agreeableness. Also, urgency cues in the emails can influence users with extraversion personality traits.

Past experiences of being a victim to phishing emails could be one of the major factors of users' susceptibility towards phishing emails. Users who were previously victim of phishing email are still influenced by authority, risk, and urgency factors. Even past experience was not helpful for them to identify the cues. Taking these into accounts, training and awareness programs should be formatted to deal with such nuances of behavioral aspects of users.

CHAPTER 5. CONCLUSION AND FUTURE WORK

In this thesis, chapter 1 explained the research problem in consideration for the study. Chapter 2 presented a detailed literature review and identified the significant gaps about the issue. Research design and methods and survey details was described in Chapter 3. In Chapter 4, data analysis results and the deductions for the effects of contextual and human factors on users' susceptibility to phishing email(s) were measured and presented. This chapter goes over the key academic and relevant contributions of this study, reviews its limitations, and presents future work.

Our main results can be summarized as follows:

- Users' characteristics such as personality traits have a significant impact on users' ability to detect phishing emails
- Users who were previously victim of phishing email are still influenced by authority, risk, and urgency factors. Even past experience was not helpful for them to identify the cues.
- Risk perception does not always have significant impact on users' susceptibility towards phishing emails
- Urgency and authority interacting together as principles of influence have a significant impact on users' susceptibility towards phishing emails
- Authority and urgency interact together to affect users' susceptibility towards phishing emails

5.1 Key academic additions

We studied the collaborative effect of the contextual and human factors and used quantitative data to recognize the influence of users' characteristics, authority, risk, urgency on users' susceptibility, in particular:

- The impact of authority, urgency and risk perception on users' susceptibility towards phishing email;
- The impact of past phishing experience on users' susceptibility to phishing email;

- The impact of human factors on users’ susceptibility; and
- the influence of personality traits on users’ susceptibility

5.2 Implications for training

To sum up, users’ susceptibility against phishing emails could potentially be upgraded by:

1. Improving users’ awareness of phishing email based cues
2. Urging users to refer an authorized person for a suspected phishing email
3. Guiding users to evaluate and respond to a suspected phishing email after careful consideration and not to be in a hurry
4. Persuading users to lower their risk-taking activities if they suspect a phishing email

5.3 Limitations of the study

In reality, individuals come across a high amount of phishing emails than we tested. The research emails, though, mocked the behavior of real phishing emails and incorporated their design features which are commonly used in most of the phishing emails. The study did not include all such features when designing the emails, and the attackers will undeniably come up with new features.

The next limitation of our study is the age of participants (18 years and older). In reality, phishing emails can reach to any user with an email address regardless of age. Young users are probably more vulnerable to phishing emails. Due to ethical issues, we restricted our study to participants aged 18 years and above.

Another important limitation is the fact that all participants were users of Amazon Mturk. The effect of this limitation could be profound as this restricts the audience.

While we conducted this study using survey, we believe doing experimental setup for this study in future can provide better nuances about these email cues and its collaborative effect as it will test these traits and factors in reality.

5.4 Recommendations for Future Research

Users come as the last element in the line of protection against phishing emails. Their defense procedure should continually be at par with the growing concerns. Even though our study identified some weaknesses in users' detection behavior and established the effect of some users' characteristics on such weaknesses, further research is needed to advance these findings and explore users' vulnerability in greater complexity.

For future work, an important experimental area is the impact of past experience of phishing email and users' capabilities to understand and detect phishing email cues. Understanding the effect of such relation with various contextual and human factors (e.g. monetary loss, emotional loss) on users' susceptibility in phishing emails would boost our knowledge repository related to users' vulnerabilities.

Based on our findings, we propose the development of a new theoretical framework understanding not only the peripheral cues but the personality, previous knowledge factors, behavioral intentions when faced with urgency, authority, risk factors. It would be an interesting study which could also investigate the collaborative effect of such cues theoretically and can guide the users with early detection of such phishing emails.

REFERENCES

A. Dijkstra, A. Rothman, and S. Pietersma. The persuasive effects of framing messages on fruit and vegetable consumption according to regulatory focus theory. Psychology & Health, 26(8):1036–1048, 2011.

Abbeel, P., Coates, A., Quigley, M., & Ng, A. Y. (2007). An application of reinforcement learning to aerobatic helicopter flight. In Advances in neural information processing systems (pp. 1-8).

Addams, J. (1914). The Larger Aspects of the Woman's Movement. The ANNALS of the American Academy of Political and Social Science, 56(1), 1–8. https://doi.org/10.1177/000271621405600101

Adorno, T., Frenkel-Brenswik, E., Levinson, D. J., & Sanford, R. N. (2019). The authoritarian personality. Verso Books.

Ajene, P. B. ANATOMY OF THE WATERING HOLE ATTACK.

Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and predicting the factors affecting end-users' risk-taking behavior. Information and Computer Security, 26(3), 306-326. doi:http://dx.doi.org.ezproxy.lib.purdue.edu/10.1108/ICS-03-2018-0037

Andersson, C., Törnberg, A., & Törnberg, P. (2014). Societal systems–complex or worse?. Futures, 63, 145-157.

Anthony Hunter. 2016. Computational Persuasion with Applications in Behaviour Change. In Computational Models of Argument - Proceedings of COMMA 2016, Potsdam, Germany, 12-16 September, 2016. 5–18.

Anti-Phishing Working Group (APWG). (2020, May 11) *Phishing Activity Trends Report 1st Quarter 2020.* https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf

Applegate, S. D. (2009). Social engineering: hacking the wetware!. Information Security Journal: A Global Perspective, 18(1), 40-46.]

Arendt, H. (1958). What is authority?. Between past and future, 91, 92.

Ashton, M. C., Lee, K., & Paunonen, S. V. (2002). What is the central feature of extraversion? Social attention versus reward sensitivity. Journal of personality and social psychology, 83(1), 245.

Barnett, J., & Breakwell, G. M. (2001). Risk perception and experience: Hazard personality profiles and individual differences. Risk Analysis, 21(1), 171-178.

Benet-Martínez, V., & John, O. P. (1998). Los Cinco Grandes across cultures and ethnic groups: Multitrait-multimethod analyses of the Big Five in Spanish and English. Journal of personality and social psychology, 75(3), 729.

Bhagyavati. (2007). "Social Engineering" in: Cyber Warfare and Cyber Terrorism, A. Colarik and L. Janczewski (eds.). Yurchak Printing Inc, New York, 182-190.

Bimal Parmar, Protecting against spear-phishing, Computer Fraud & Security, Volume 2012, Issue 1, 2012, Pages 8-11, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(12)70007-6

Bleidorn, W., & Hopwood, C. J. (2019). Using machine learning to advance personality assessment and theory. Personality and Social Psychology Review, 23(2), 190-203.

Bong-Goon Seo, Do-Hyung Park, The effect of message framing on security behavior in online services: Focusing on the shift of time orientation via psychological ownership, Computers in Human Behavior, Volume 93, 2019, Pages 357-369, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2018.12.035.

Breda, Filipe & Barbosa, Hugo & Morais, Telmo. (2017). SOCIAL ENGINEERING AND CYBER SECURITY. 4204-4211. 10.21125/inted.2017.1008.

Bromiley, P., & Curley, S. P. (1992). Individual differences in risk taking.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks—A literature-based dissection of successful attacks. Journal of investigative psychology and offender profiling, 15(1), 20-45.

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.

C. A. Godinho, M.-J. Alvarez, and M. L. Lima. Emphasizing the losses or the gains: Comparing situational and individual moderators of framed messages to promote fruit and vegetable intake. Appetite, 96:416 – 425, 2016.

Campbell, Andrew & Cumming, Steven & Hughes, Ian. (2006). Internet Use by the Socially Fearful: Addiction or Therapy?. Cyberpsychology & behavior : the impact of the Internet, multimedia and virtual reality on behavior and society. 9. 69-81. 10.1089/cpb.2006.9.69.

Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. Computers in human behavior, 23(3), 1273-1284.

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. Human factors, 58(8), 1158-1172.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2013). Going spear phishing: Exploring embedded training and awareness. IEEE Security & Privacy, 12(1), 28-38.

Chandler, J., Rosenzweig, C., Moss, A.J. et al. Online panels in social science research: Expanding sampling methods beyond Mechanical Turk. Behav Res 51, 2022–2038 (2019). https://doi.org/10.3758/s13428-019-01273-7

Cialdini, R. B. (1993). Influence: The psychology of persuasion (Rev. ed.). New York: Morrow.

Cialdini, R. B. (2001) Influence: Science and practice, Pearson Education, Massachusetts.

Cialdini, R. B. (2009). Influence: Science and practice (Vol. 4). Boston: Pearson education.

Cole, E., & Ring, S. (2005). Insider threat: Protecting the enterprise from sabotage, spying, and theft. Elsevier.

Cone B.D., Thompson M.F., Irvine C.E., Nguyen T.D. (2006) Cyber Security Training and Awareness Through Game Play. In: Fischer-Hübner S., Rannenberg K., Yngström L., Lindskog S. (eds) Security and Privacy in Dynamic Environments. SEC 2006. IFIP International Federation for Information Processing, vol 201. Springer, Boston, MA

Cusack, B., & Adedokun, K. (2018). The impact of personality traits on user's susceptibility to social engineering attacks.

D. N. Walton and C. A. Reed. Argumentation schemes and defeasible inferences. In 15th European Conference on Artificial Intelligence. ECAI 2002., 2002.

D. Walton, C. Reed, and F. Macagno. Argumentation schemes. Cambridge University Press, 2008.

Darren Duxbury, Barbara Summers, Financial risk perception: Are individuals variance averse or loss averse?, Economics Letters Volume 84, Issue 1, 2004, Pages 21-28, ISSN 0165-1765, https://doi.org/10.1016/j.econlet.2003.12.006.

Darwish, A., Zarka, A., & Aloul, F. (2012). Towards understanding phishing victims' profile. 2012 International Conference on Computer Systems and Industrial Informatics, 1-5.

Davinson, N., & Sillence, E. (2014). Using the health belief model to explore users' perceptions of ‘being safe and secure’in the world of technology mediated financial transactions. International Journal of Human-Computer Studies, 72(2), 154-168.

Davis, K. (1937). The sociology of prostitution. American Sociological Review, 2(5), 744-755.

Denning, P. J., & Denning, D. E. (2016). Cybersecurity is harder than building bridges. American Scientist, 104(3), 155.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems (pp. 581-590).

Di, W., Peng, G., & Jichang, D. (2011). Game-theory-based Analysis of and Proposed Solution to the Indemnificatory Housing Lease Default Problem [J]. Management Review, 2

Dillman, D. A. (2011). Mail and Internet surveys: The tailored design method--2007 Update with new Internet, visual, and mixed-mode guide. John Wiley & Sons. doi: 10.1109/COMPSAC.2016.105 doi: 10.1109/ISSA.2010.5588500

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006, July). Decision strategies and susceptibility to phishing. In Proceedings of the second symposium on Usable privacy and security (pp. 79-90).
Duxbury, D., & Summers, B. (2004). Financial risk perception: Are individuals variance averse or loss averse?. Economics Letters, 84(1), 21-28.

E. T. Higgins. Beyond pleasure and pain. American Psychologist, 52(12):1280–1300, dec 1997

Eagly, A. H., & Chaiken, S. (1993). The psychology of attitudes. Harcourt brace Jovanovich college publishers.

Emerson, R. M. (1976). Social exchange theory. Annual review of sociology, 2(1), 335-362.

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations:(IR) relevant theory?. International political science review, 27(3), 221-244.

Ermer, E., Cosmides, L., & Tooby, J. (2008). Relative status regulates risky decision making about resources in men: Evidence for the co-evolution of motivation and cognition. Evolution and Human Behavior, 29(2), 106-118.

Ferreira, A., Coventry, L., & Lenzini, G. (2015, August). Principles of persuasion in social engineering and their use in phishing. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 36-47). Springer, Cham.

Fink, A. (2015). How to conduct surveys: A step-by-step guide. Sage Publications.

Framing. (n.d.) Retrieved from https://www.social-engineer.org/framework/influencing-others/framing/

Goldberg, L. R. (1993). The structure of phenotypic personality traits. American psychologist, 48(1), 26.

Gragg D. A Multi-Level Defense Against Social Engineering. SANS Instit InfoSec Read Room 2003;1–21.

Greiner, L. (2006). Hacking your network's weakest link: you. netWorker, 12(1), 9-11.

Guéguen, N., & Jacob, C. (2002). Solicitation by e-mail and solicitor's status: A field study of social influence on the web. CyberPsychology & Behavior, 5(4), 377-383.

Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015).

Halevi, Tzipora & Lewis, Jim & Memon, Nasir. (2013). Phishing, Personality Traits and Facebook.

Halevi, Tzipora & Memon, Nasir & Nov, Oded. (2015). Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. SSRN Electronic Journal. 10.2139/ssrn.2544742.

Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. Computers & Security, 24(1), 31-43.

Hauben, M. (2007). History of ARPANET. Site de l'Instituto Superior de Engenharia do Porto, 17.

Haugen, R. A. (1995). The new finance: the case against efficient markets. Prentice Hall.

Hill, C. A., & O'Hara, E. A. (2006). A cognitive theory of trust. Wash. UL Rev., 84, 1717.

Hirsh, J. B., Kang, S. K., & Bodenhausen, G. V. (2012). Personalized persuasion: Tailoring persuasive appeals to recipients' personality traits. Psychological science, 23(6), 578-581.

Huber M, Mulazzani M, Kitzler G, Goluch S,Weippl E. Friend-inthe-middle attacks: exploiting social networking sites for spam. IEEE Internet Comput 2011;15(3):28–34.

Ivaturi, K., & Janczewski, L. (2011, June). A taxonomy for social engineering attacks. In International Conference on Information Resources Management (pp. 1-12). Centre for Information Technology, Organizations, and People.

J. Campbell, N. Greenauer, K. Macaluso, and C. End. Unrealistic optimism in internet events. Computers in Human Behavior, 23:1273–1284, 2007.

Jacob Hirsh, Sonia K Kang, and Galen Bodenhausen. 2012. Personalized Persuasion: Tailoring Persuasive Appeals to Recipients' Personality Traits. Psychological science 23 (04 2012), 578–81.

Janis, I. L. (1954). Personality Correlates of Susceptibility To Persuasion 1. Journal of personality, 22(4), 504-518.

Jhaveri, H., Jhaveri, H., & Sanghavi, D. (2014). Sybil attack and its proposed solution. International Journal of Computer Applications, 105(3).

John, O. P., Robins, R. W., & Pervin, L. A. (Eds.). (2010). Handbook of personality: Theory and research. Guilford Press.

Johnson, J. A. (2014). Measuring thirty facets of the Five Factor Model with a 120-item public domain inventory: Development of the IPIP-NEO-120. Journal of Research in Personality, 51, 78-89.

Josekutty Thomas, R. (2019). Personalised persuasive messages for behaviour change interventions: combining Cialdini's principles and argumentation schemes (Doctoral dissertation, University of Aberdeen).

Joseph M. Hatfield, Social engineering in cybersecurity: The evolution of a concept, Computers & Security, Volume 73, 2018, Pages 102-113, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2017.10.008

Julie S. Downs, Mandy Holbrook, and Lorrie Faith Cranor. 2007. Behavioral response to phishing risk. In Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit (eCrime '07). Association for Computing Machinery, New York, NY, USA, 37–44. DOI:https://doi-org.ezproxy.lib.purdue.edu/10.1145/1299015.1299019

Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1990). Experimental tests of the endowment effect and the Coase theorem. Journal of political Economy, 98(6), 1325-1348.

Kamal, M., & Crews, D. (2008). The psychology of IT security in business. Journal of American Academy of Business, 13(1), 145-150.

Kennedy, A. and Parsons, A. (2014), "Social engineering and social marketing: why is one “good” and the other “bad”?", Journal of Social Marketing, Vol. 4 No. 3, pp. 198-209. https://doi.org/10.1108/JSOCM-01-2014-0006

Kumaraguru, P., Acquisti, A., & Cranor, L. F. (2006, October). Trust modelling for online transactions: a phishing scenario. In Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services (pp. 1-9).

Lauinger, T., Pankakoski, V., Balzarotti, D., & Kirda, E. (2010, April). Honeybot, Your Man in the Middle for Automated Social Engineering. In LEET.

Lavine, H., Burgess, D., Snyder, M., Transue, J., Sullivan, J. L., Haney, B., & Wagner, S. H. (1999). Threat, authoritarianism, and voting: An investigation of personality and persuasion. Personality and Social Psychology Bulletin, 25(3), 337-347.

Levin, I. P., Schneider, S. L., & Gaeth, G. J. (1998). All frames are not created equal: A typology and critical analysis of framing effects. Organizational behavior and human decision processes, 76(2), 149-188.

Lim, K. H., Lim, E. P., Jiang, B., & Achananuparp, P. (2016, July). Using online controlled experiments to examine authority effects on user behavior in email campaigns. In Proceedings of the 27th ACM Conference on Hypertext and Social Media (pp. 255-260). ACM.

Lindqvist, U., & Jonsson, E. (1997, May). How to systematically classify computer security intrusions. In Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097) (pp. 154-163). IEEE.

M. Bezuidenhout, F. Mouton and H. S. Venter, "Social engineering attack detection model: SEADM," 2010 Information Security for South Africa, Sandton, Johannesburg, 2010, pp. 1-8.

M. Donnellan, F. Oswald, B. Baird, and R. Lucas. The mini-IPIP scales: Tiny-yet-effective measures of the Big Five factors of personality. Psychological Assessment, 18(2):192–203, 2006.

Maheshwari, S. (2011). SECURITY ISSUES IN BANKING & FINANCIAL SECTOR. International Journal of Advanced Research in Computer Science, 2(1) Retrieved from https://search.proquest.com/docview/1443705607?accountid=13360

Manske, K. (2000). An Introduction to Social Engineering. Information Security Journal: A Global Perspective, 9(5), 1-7.

McCrae, R. R., & Costa, P. T. (1999). Handbook of personality theory and research (Vol. 2). New York, NY: Guilford.

Michael Workman Ph.D. (2007) Gaining Access with Social Engineering: An Empirical Study of the Threat, Information Systems Security, 16:6, 315-331, DOI: 10.1080/10658980701788165

Milgram, S. (1974). Obedience to authority. Harper.

Mishra, S. (2014). Decision-making under risk: Integrating perspectives from biology, economics, and psychology. Personality and Social Psychology Review, 18(3), 280-307.

Mishra, S., & Lalumière, M. L. (2008). Risk-taking, antisocial behavior, and life histories. Evolutionary forensic psychology, 139-159.

Mitnick, K. D., & Simon, W. L. (2003). The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons.

Monica Lagazio, Nazneen Sherif, Mike Cushman, A multi-level approach to understanding the impact of cyber crime on the financial sector, Computers & Security, Volume 45, 2014, Pages 58-74, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2014.05.006.

Nalin Asanka Gamagedara Arachchilage, Steve Love, A game design framework for avoiding phishing attacks, Computers in Human Behavior, Volume 29, Issue 3, 2013, Pages 706-714, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2012.12.018.

Ozkaya, E., & Safari, an O’Reilly Media Company. (2018). Learn Social Engineering (1st ed.).
Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. International Journal of Human-Computer Studies, 128, 17-26.

Payne, J. W. (1975). Relation of perceived risk to preferences among gambles. Journal of Experimental Psychology: Human Perception and Performance, 1(1), 86.

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. In Communication and persuasion (pp. 1-24). Springer, New York, NY.

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

Rui Chen, Joana Gaia, H. Raghav Rao, An examination of the effect of recent phishing encounters on phishing susceptibility, Decision Support Systems, Volume 133, 2020, 113287, ISSN 0167-9236, https://doi.org/10.1016/j.dss.2020.113287.

S. Duman, K. Kalkan-Cakmakci, M. Egele, W. Robertson and E. Kirda, "EmailProfiler: Spearphishing Filtering with Header and Stylometric Features of Emails," 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, 2016, pp. 408-416.

Saleem, Jibran & Hammoudeh, Mohammad. (2018). Defense Methods Against Social Engineering Attacks. 10.1007/978-3-319-58424-9_35.

Schneier, B. (2006). Beyond fear: Thinking sensibly about security in an uncertain world. Springer Science & Business Media.

Schrammel, Johann & Hochleitner, Christina & Tscheligi, Manfred. (2009). Personality Traits, Usage Patterns and Information Disclosure in Online Communities. 10.14236/ewic/HCI2009.19.

Sen, S., & Airiau, S. (2007). IJCAI International Joint Conference on Artificial Intelligence, 1507 1512.

Shi, Z. R., Schlenker, A., Hay, B., & Fang, F. Draining the Water Hole: Mitigating Social Engineering Attacks.

Shmueli-Scheuer, M., Herzig, J., Konopnicki, D., & Sandbank, T. (2019, June). Detecting Persuasive Arguments based on Author-Reader Personality Traits and their Interaction. In Proceedings of the 27th ACM Conference on User Modeling, Adaptation and Personalization (pp. 211-215). ACM.

Simkins, C., Isbell, C., & Marquez, N. (2010, August). Deriving behavior from personality: a reinforcement learning approach. In International Conference on Cognitive Modelling (pp. 229-234).

Slade, J. A. (1929). Law and psychology. The Journal of Abnormal and Social Psychology, 24(2), 212.

Slovic, P., & Lichtenstein, S. (1968). Relative importance of probabilities and payoffs in risk taking. Journal of experimental psychology, 78(3p2), 1.

Smith, S. M., & Petty, R. E. (1996). Message framing and persuasion: A message processing analysis. Personality and Social Psychology Bulletin, 22(3), 257-268.

Stajano, F., & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. Communications of the ACM, 54(3), 70-75.

Sunstein, C. R. (2005). Moral heuristics. Behavioral and brain sciences, 28(4), 531-541.

Sussman, S. W., & Siegal, W. S. (2003). Informational influence in organizations: An integrated approach to knowledge adoption. Information systems research, 14(1), 47-65.

Thornburgh, T. (2004, October). Social engineering: the dark art. In Proceedings of the 1st annual conference on Information security curriculum development (pp. 133-135). ACM.

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. Science, 211(4481), 453-458.

Uebelacker, S., & Quiel, S. (2014, July). The social engineering personality framework. In 2014 Workshop on Socio-Technical Aspects in Security and Trust (pp. 24-30). IEEE.

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. Communication Research, 45(8), 1146-1166.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576-586.

Walker, M. A. (2000). An application of reinforcement learning to dialogue strategy selection in a spoken dialogue system for email. Journal of Artificial Intelligence Research, 12, 387-416.

Wang, Y. C., & Usher, J. M. (2005). Application of reinforcement learning for agent-based production scheduling. Engineering Applications of Artificial Intelligence, 18(1), 73-82.

Weber, E. U., Blais, A. R., & Betz, N. E. (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. Journal of behavioral decision making, 15(4), 263-290.

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. International Journal of Human-Computer Studies, 120, 1-13.

Workman, M. (2008). A test of interventions for security threats from social engineering. Information Management & Computer Security.

Yang, G. H., & Yu, Y. (2018). Use of Interpersonal Deception Theory in Counter Social Engineering. In Proceedings of the 2nd International Workshop on Rumours and Deception in Social Media.

Young, K. S., & De Abreu, C. N. (2011). Internet addiction. A handbook and guide to evaluation.
Zhang, W., & Watts, S. (2008). Online communities as communities of practice: a case study. Journal of Knowledge Management.

Zheng, L., Goldberg, L. R., Zheng, Y., Zhao, Y., Tang, Y., & Liu, L. (2008). Reliability and Concurrent Validation of the IPIP Big-Five Factor Markers in China: Consistencies in Factor Structure between Internet-Obtained Heterosexual and Homosexual Samples. Personality and individual differences, 45(7), 649–654. https://doi.org/10.1016/j.paid.2008.07.009

Zhengxing Huang, W.M.P. van der Aalst, Xudong Lu, Huilong Duan, Reinforcement learning based resource allocation in business process management, Data & Knowledge Engineering, Volume 70, Issue 1, 2011, Pages 127-145, ISSN 0169-023X, https://doi.org/10.1016/j.datak.2010.09.002.

APPENDIX A: RESEARCH SURVEY

1. Gender:

□ Male □ Female □ Other

2. Ethnicity:

□ White □ Black or African American □ American Indian or Alaska Native

□ Asian □ Native Hawaiian or Pacific Islander □ Other

3. Age:

□ 18-24 □ 25-29 □ 30-34 □ 34-39 □ 40-44 □ 45-49 □ 50-54

□ 55-59 □ 60-64 □ 65-69 □ 70 or older

4. Please circle the corresponding number in each statement which best describes the degree to which a statement is true for you:

Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly Agree
1	2	3	4	5

5. I am someone who:

would never go hang gliding or bungee jumping	1	2	3	4	5
would never make a high risk investment	1	2	3	4	5
avoids dangerous situations	1	2	3	4	5
seeks danger	1	2	3	4	5
enjoys being reckless	1	2	3	4	5

6. In an average week how many hours do you spend online for:

□ Work

□ Leisure

□ Other

7. Have you ever fallen victim to a phishing email?

□ Yes □ No □ I don't know

8. What were the consequences for you of falling for a phishing email? (select all that apply)

□ I lost a little money (<$500) □ I lost a great deal of money (> $500)

□ I had to change my login information □ I lost control of my account(s)

□ My identity was stolen

□ My company was negatively impacted

□ I was the victim of ransomware

□ My reputation was damaged

□ My computer was infected with a virus

□ There were no consequences

□ Other

9. I see myself as someone who:

Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly Agree
1	2	3	4	5

Is talkative	1	2	3	4	5
Tends to find fault with other	1	2	3	4	5
Does a thorough job	1	2	3	4	5
Is depressed, blue	1	2	3	4	5
Is original, comes up with new ideas	1	2	3	4	5
Is reserved	1	2	3	4	5
Is helpful and unselfish with others	1	2	3	4	5
Can be somewhat careless	1	2	3	4	5

Is relaxed, handles stress well	1	2	3	4	5
Is curious about many different things	1	2	3	4	5
Is full of energy	1	2	3	4	5
Starts quarrels with others	1	2	3	4	5
Is a reliable worker	1	2	3	4	5
Can be tense	1	2	3	4	5
Is ingenious, a deep thinker	1	2	3	4	5
Generates a lot of enthusiasm	1	2	3	4	5

Has a forgiving nature	1	2	3	4	5
Tends to be disorganized	1	2	3	4	5
Worries a lot	1	2	3	4	5
Has an active imagination	1	2	3	4	5
Tends to be quiet	1	2	3	4	5
Is generally trusting	1	2	3	4	5
Tends to be lazy	1	2	3	4	5
Is emotionally stable, not easily upset	1	2	3	4	5

Is inventive	1	2	3	4	5
Has an assertive personality	1	2	3	4	5
Can be cold and aloof	1	2	3	4	5
Perseveres until the task is finished	1	2	3	4	5
Can be moody	1	2	3	4	5
Values artistic, aesthetic experiences	1	2	3	4	5
Is sometimes shy, inhibited	1	2	3	4	5
Is considerate and kind to almost everyone	1	2	3	4	5

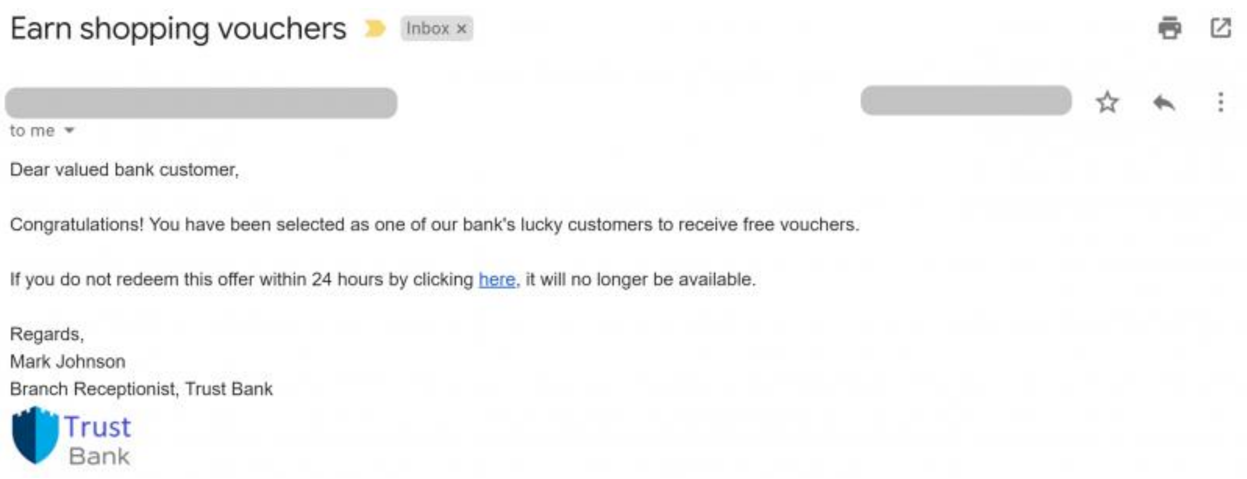
Does things efficiently	1	2	3	4	5
Remains calm in tense situations	1	2	3	4	5
Prefers work that is routine	1	2	3	4	5
Is outgoing, sociable	1	2	3	4	5
Is sometimes rude to others	1	2	3	4	5
Makes plans and follows through with them	1	2	3	4	5
Gets nervous easily	1	2	3	4	5
Likes to reflect, play with ideas	1	2	3	4	5

Has few artistic interests	1	2	3	4	5
Likes to cooperate with others	1	2	3	4	5

Is easily distracted	1	2	3	4	5
Is sophisticated in art, music, or literature	1	2	3	4	5

For the next set of questions you will see a series of emails. Some of them are phishing emails and some of them are genuine. Please indicate how likely you

11. Please read the following email to answer the question.



Earn shopping vouchers

[redacted] [redacted]

to me

Dear valued bank customer,

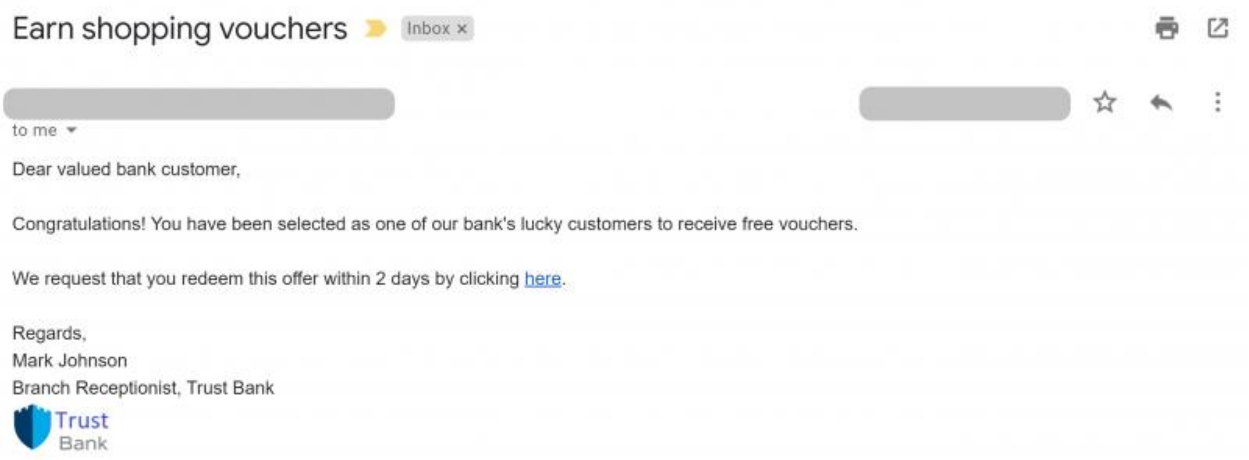
Congratulations! You have been selected as one of our bank's lucky customers to receive free vouchers.

If you do not redeem this offer within 24 hours by clicking here, it will no longer be available.

Regards,
Mark Johnson
Branch Receptionist, Trust Bank
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

12. Please read the following email to answer the question.



Earn shopping vouchers

[redacted] [redacted]

to me

Dear valued bank customer,

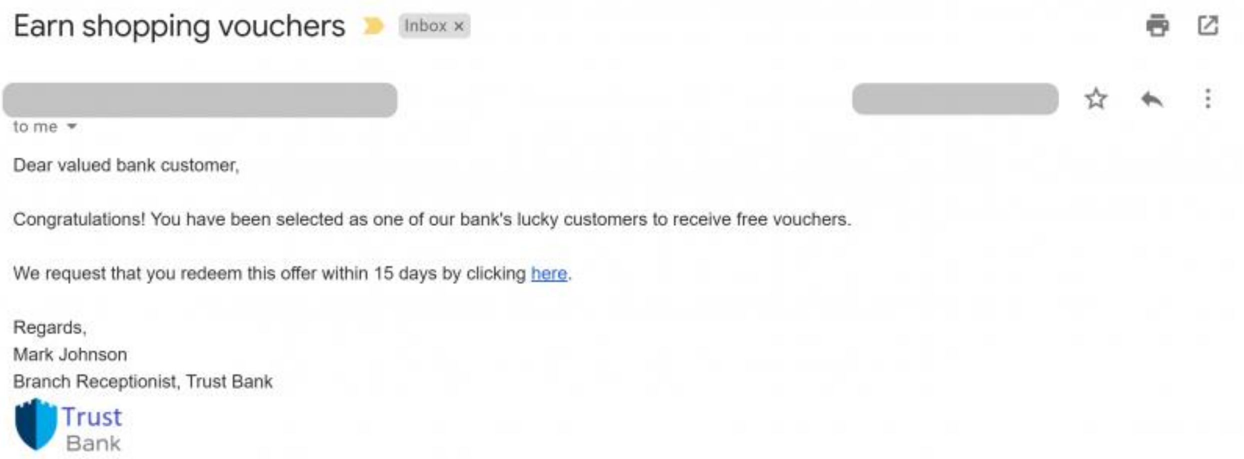
Congratulations! You have been selected as one of our bank's lucky customers to receive free vouchers.

We request that you redeem this offer within 2 days by clicking here.

Regards,
Mark Johnson
Branch Receptionist, Trust Bank
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

13. Please read the following email to answer the question.



Earn shopping vouchers

[redacted] [redacted]

to me

Dear valued bank customer,

Congratulations! You have been selected as one of our bank's lucky customers to receive free vouchers.

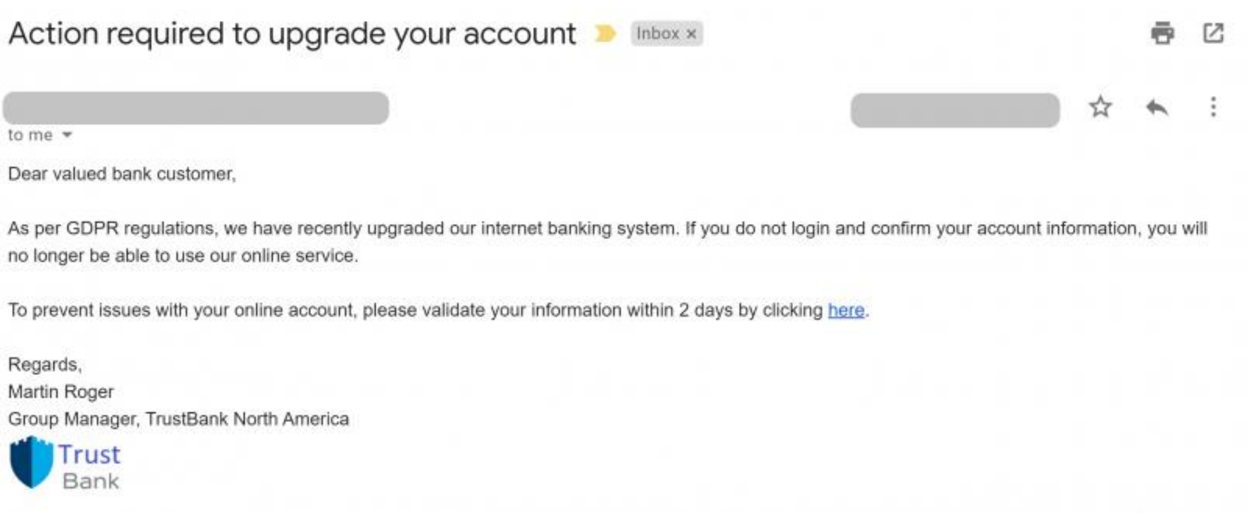
We request that you redeem this offer within 15 days by clicking here.

Regards,
Mark Johnson
Branch Receptionist, Trust Bank
Trust
Bank

	Extremely	Somewhat	Neither	Somewhat	Extremely

	unlikely	unlikely	likely nor unlikely	likely	likely
How likely are you to click on the link?	□	□	□	□	□

14. Please read the following email to answer the question.



Action required to upgrade your account

[redacted]

[redacted]

Dear valued bank customer,

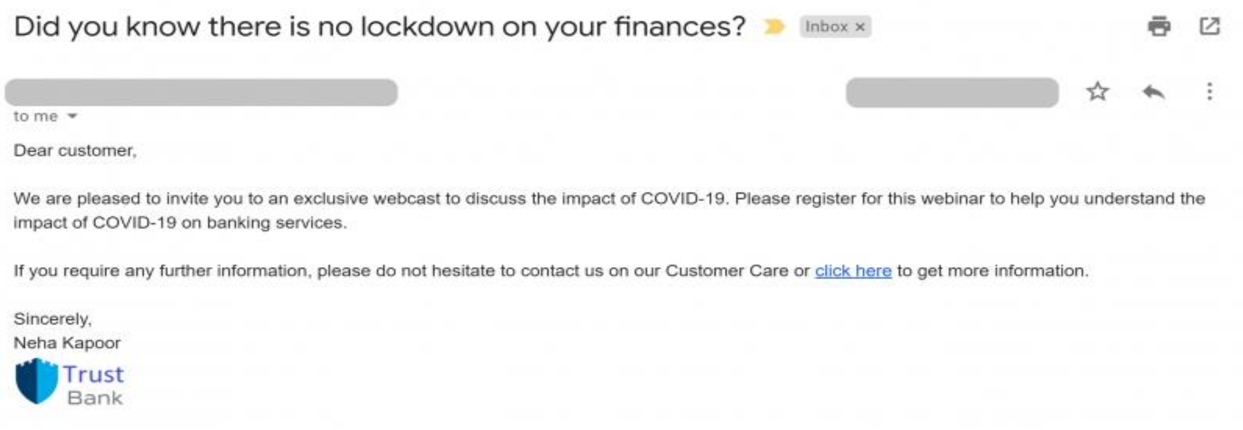
As per GDPR regulations, we have recently upgraded our internet banking system. If you do not login and confirm your account information, you will no longer be able to use our online service.

To prevent issues with your online account, please validate your information within 2 days by clicking here.

Regards,
Martin Roger
Group Manager, TrustBank North America
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

15. Please read the following email to answer the question.



Did you know there is no lockdown on your finances?

[redacted]

[redacted]

Dear customer,

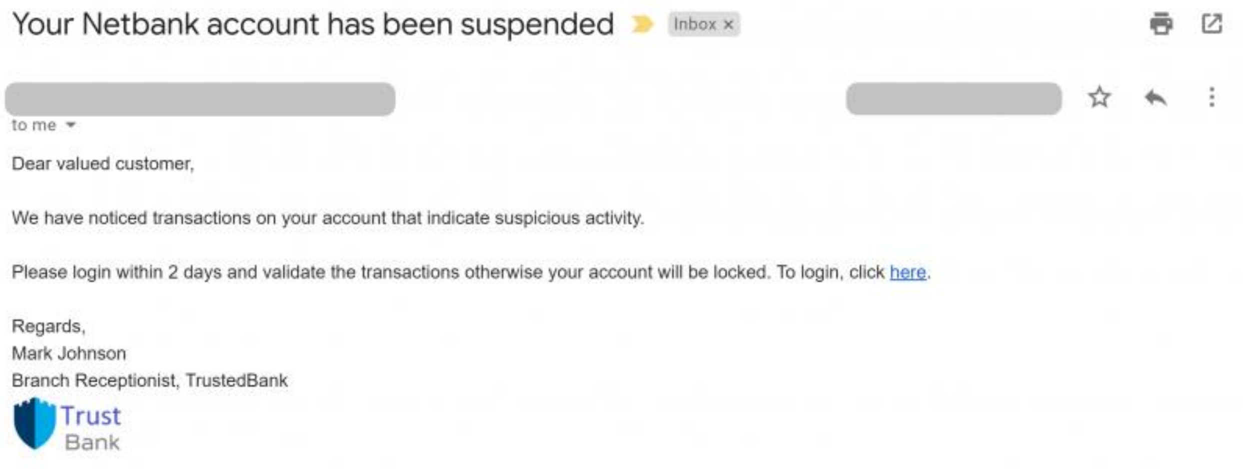
We are pleased to invite you to an exclusive webcast to discuss the impact of COVID-19. Please register for this webinar to help you understand the impact of COVID-19 on banking services.

If you require any further information, please do not hesitate to contact us on our Customer Care or click here to get more information.

Sincerely,
Neha Kapoor
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

16. Please read the following email to answer the question.



Your Netbank account has been suspended

[redacted]

[redacted]

Dear valued customer,

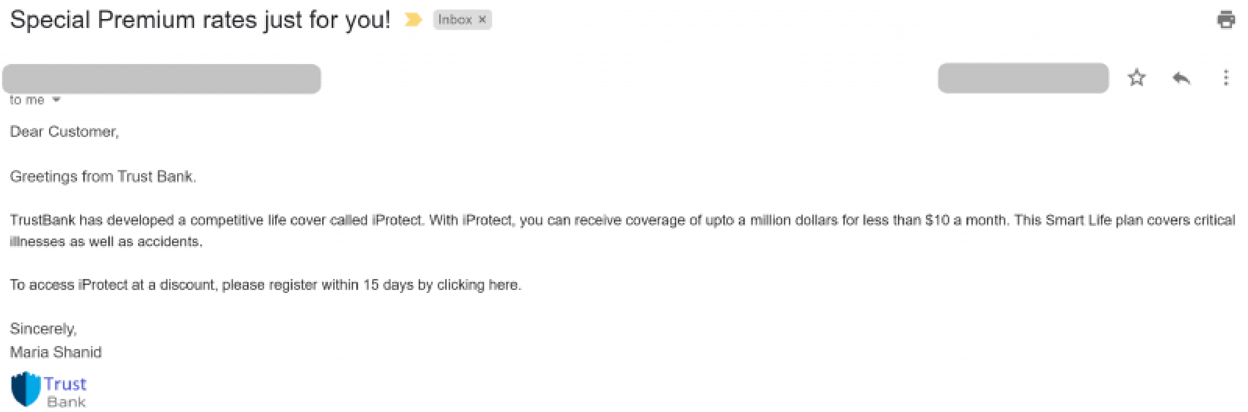
We have noticed transactions on your account that indicate suspicious activity.

Please login within 2 days and validate the transactions otherwise your account will be locked. To login, click here.

Regards,
Mark Johnson
Branch Receptionist, TrustedBank
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

17. Please read the following email to answer the question.



Special Premium rates just for you!

[redacted]

[redacted]

Dear Customer,

Greetings from Trust Bank.

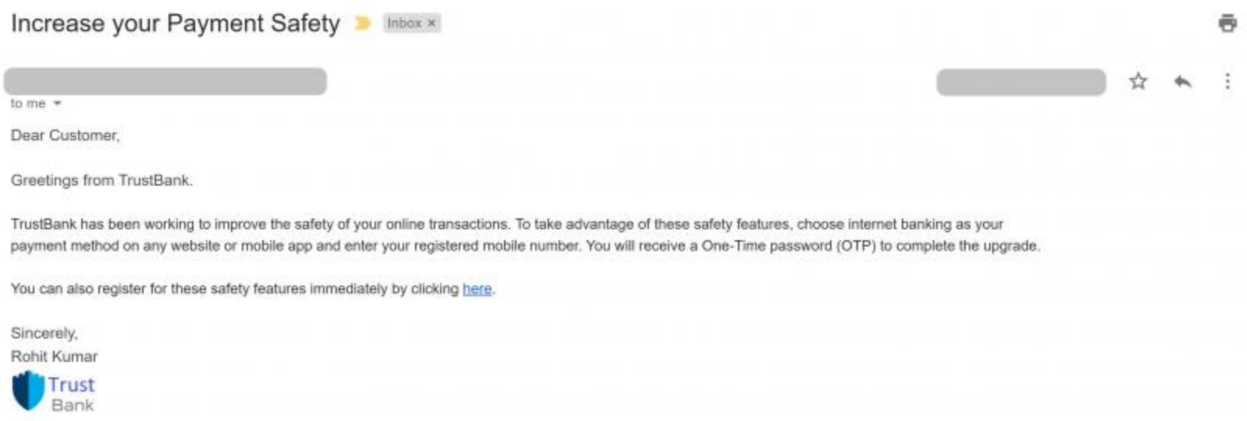
TrustBank has developed a competitive life cover called iProtect. With iProtect, you can receive coverage of upto a million dollars for less than $10 a month. This Smart Life plan covers critical illnesses as well as accidents.

To access iProtect at a discount, please register within 15 days by clicking here.

Sincerely,
Maria Shanid

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

18. Please read the following email to answer the question.



Increase your Payment Safety

[redacted] [redacted]

Dear Customer,

Greetings from TrustBank.

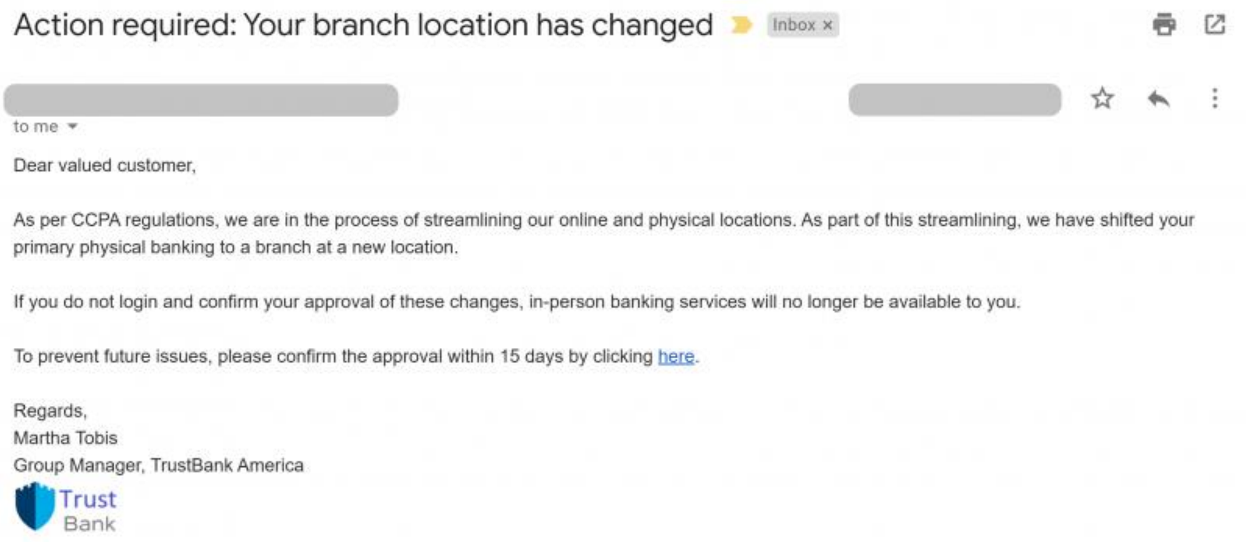
TrustBank has been working to improve the safety of your online transactions. To take advantage of these safety features, choose internet banking as your payment method on any website or mobile app and enter your registered mobile number. You will receive a One-Time password (OTP) to complete the upgrade.

You can also register for these safety features immediately by clicking here.

Sincerely,
Rohit Kumar
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

19. Please read the following email to answer the question.



Action required: Your branch location has changed

[redacted] [redacted]

Dear valued customer,

As per CCPA regulations, we are in the process of streamlining our online and physical locations. As part of this streamlining, we have shifted your primary physical banking to a branch at a new location.

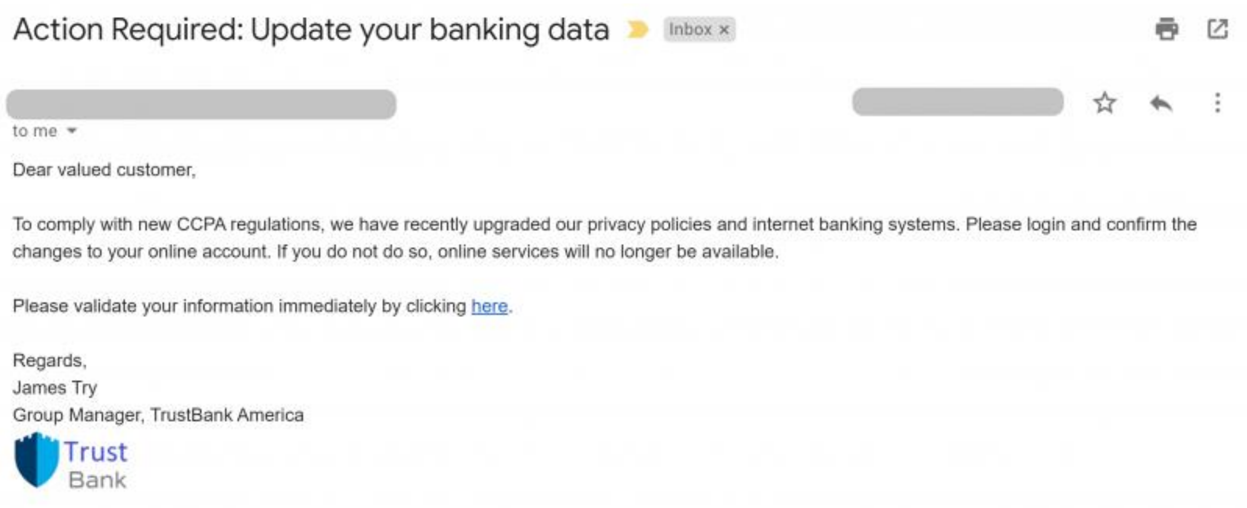
If you do not login and confirm your approval of these changes, in-person banking services will no longer be available to you.

To prevent future issues, please confirm the approval within 15 days by clicking here.

Regards,
Martha Tobis
Group Manager, TrustBank America
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

20. Please read the following email to answer the question.



Action Required: Update your banking data

[redacted] [redacted]

Dear valued customer,

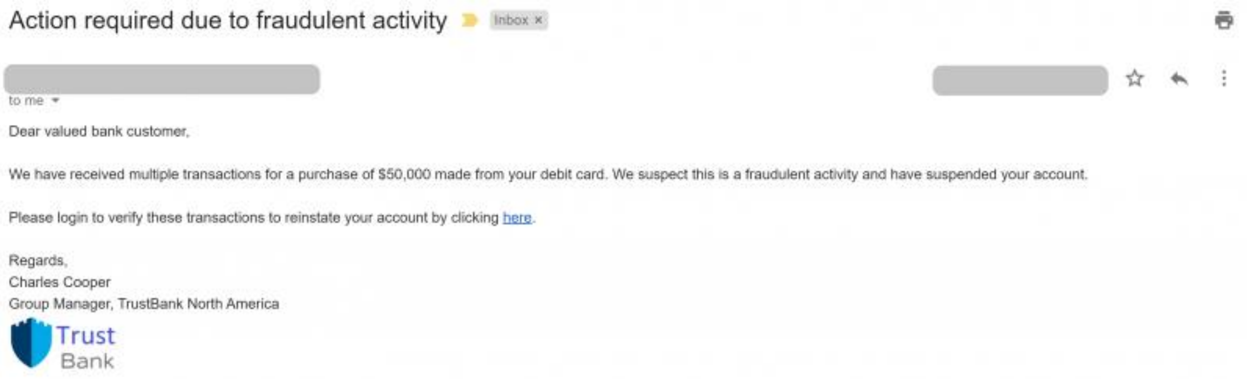
To comply with new CCPA regulations, we have recently upgraded our privacy policies and internet banking systems. Please login and confirm the changes to your online account. If you do not do so, online services will no longer be available.

Please validate your information immediately by clicking here.

Regards,
James Try
Group Manager, TrustBank America

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

21. Please read the following email to answer the question.



Action required due to fraudulent activity

[redacted] [redacted]

Dear valued bank customer,

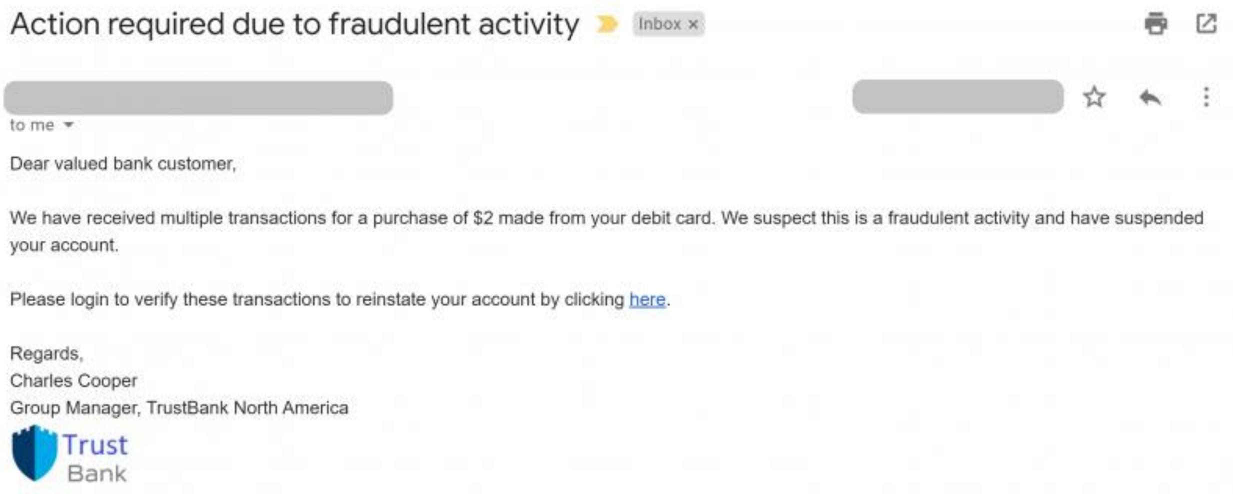
We have received multiple transactions for a purchase of $50,000 made from your debit card. We suspect this is a fraudulent activity and have suspended your account.

Please login to verify these transactions to reinstate your account by clicking here.

Regards,
Charles Cooper
Group Manager, TrustBank North America
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

22. Please read the following email to answer the question.



Action required due to fraudulent activity

[redacted] [redacted]

Dear valued bank customer,

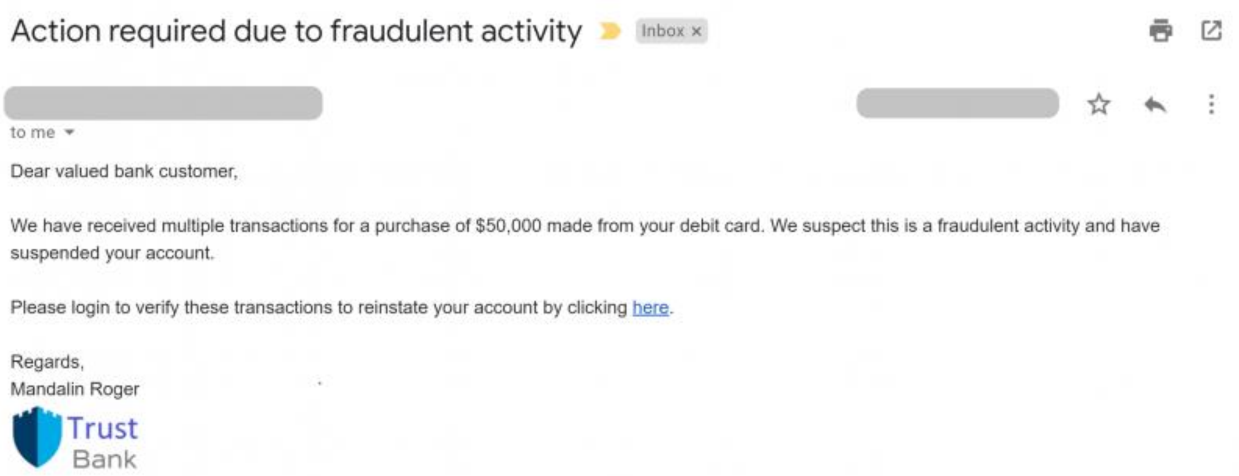
We have received multiple transactions for a purchase of $2 made from your debit card. We suspect this is a fraudulent activity and have suspended your account.

Please login to verify these transactions to reinstate your account by clicking here.

Regards,
Charles Cooper
Group Manager, TrustBank North America
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

23. Please read the following email to answer the question.



Action required due to fraudulent activity

Dear valued bank customer,

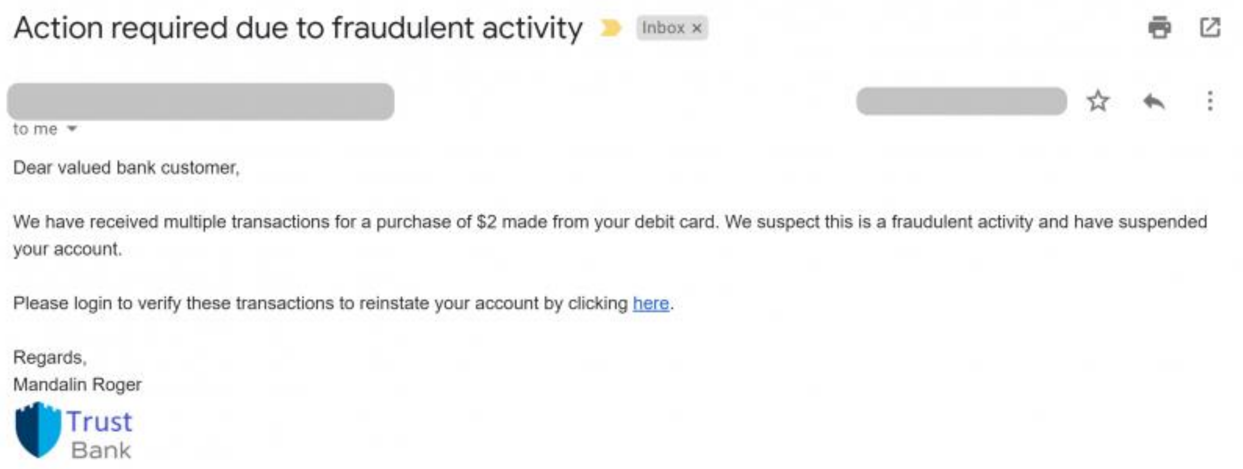
We have received multiple transactions for a purchase of $50,000 made from your debit card. We suspect this is a fraudulent activity and have suspended your account.

Please login to verify these transactions to reinstate your account by clicking here.

Regards,
Mandalin Roger

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

24. Please read the following email to answer the question.



Action required due to fraudulent activity

[redacted] [redacted]

to me

Dear valued bank customer,

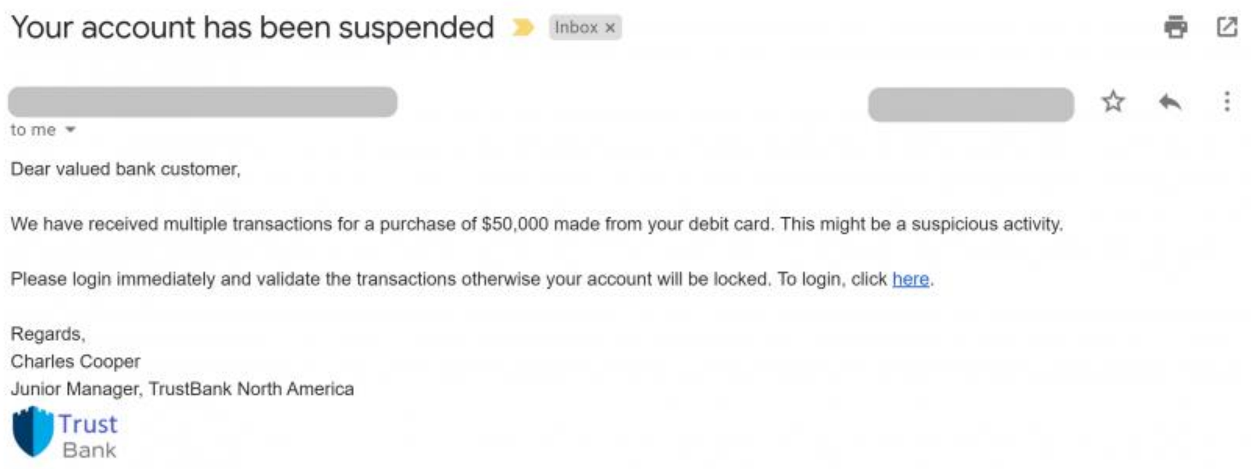
We have received multiple transactions for a purchase of $2 made from your debit card. We suspect this is a fraudulent activity and have suspended your account.

Please login to verify these transactions to reinstate your account by clicking here.

Regards,
Mandalin Roger
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

25. Please read the following email to answer the question.



Your account has been suspended

[redacted] [redacted]

to me

Dear valued bank customer,

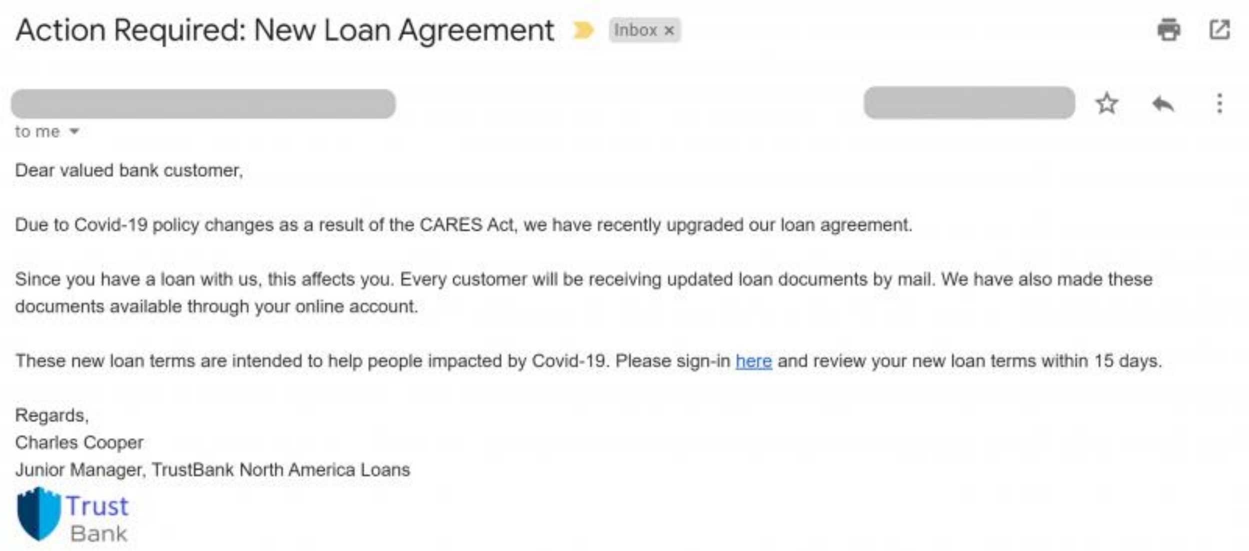
We have received multiple transactions for a purchase of $50,000 made from your debit card. This might be a suspicious activity.

Please login immediately and validate the transactions otherwise your account will be locked. To login, click here.

Regards,
Charles Cooper
Junior Manager, TrustBank North America
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

26. Please read the following email to answer the question.



Action Required: New Loan Agreement

[redacted]

[redacted]

Dear valued bank customer,

Due to Covid-19 policy changes as a result of the CARES Act, we have recently upgraded our loan agreement.

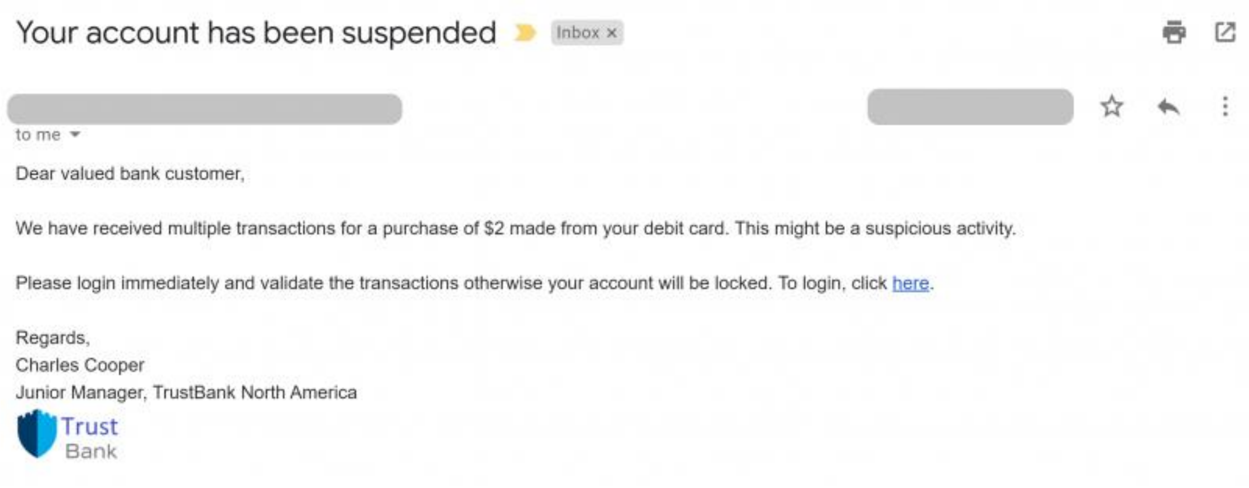
Since you have a loan with us, this affects you. Every customer will be receiving updated loan documents by mail. We have also made these documents available through your online account.

These new loan terms are intended to help people impacted by Covid-19. Please sign-in here and review your new loan terms within 15 days.

Regards,
Charles Cooper
Junior Manager, TrustBank North America Loans

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

27. Please read the following email to answer the question.



Your account has been suspended

[redacted] [redacted]

to me

Dear valued bank customer,

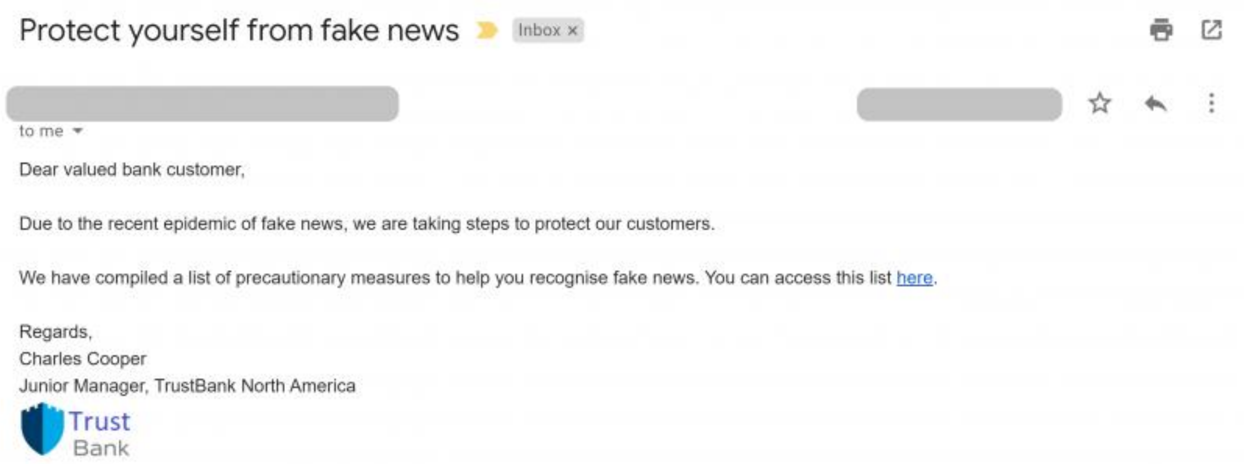
We have received multiple transactions for a purchase of $2 made from your debit card. This might be a suspicious activity.

Please login immediately and validate the transactions otherwise your account will be locked. To login, click here.

Regards,
Charles Cooper
Junior Manager, TrustBank North America
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

28. Please read the following email to answer the question.



Protect yourself from fake news

[redacted] [redacted]

to me

Dear valued bank customer,

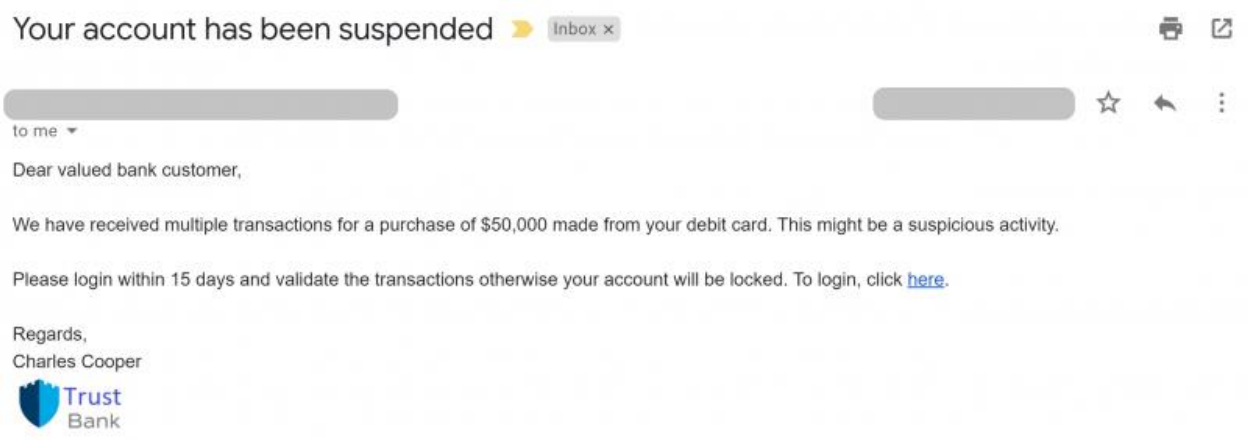
Due to the recent epidemic of fake news, we are taking steps to protect our customers.

We have compiled a list of precautionary measures to help you recognise fake news. You can access this list here.

Regards,
Charles Cooper
Junior Manager, TrustBank North America
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

29. Please read the following email to answer the question.



Your account has been suspended

[redacted] [redacted]

to me

Dear valued bank customer,

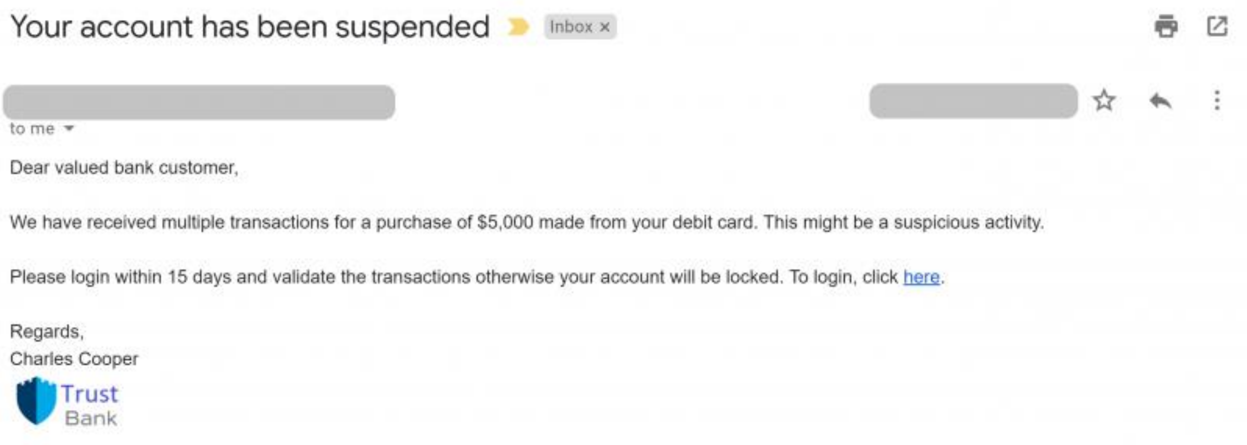
We have received multiple transactions for a purchase of $50,000 made from your debit card. This might be a suspicious activity.

Please login within 15 days and validate the transactions otherwise your account will be locked. To login, click here.

Regards,
Charles Cooper
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

30. Please read the following email to answer the question.



Your account has been suspended

[redacted] [redacted]

to me

Dear valued bank customer,

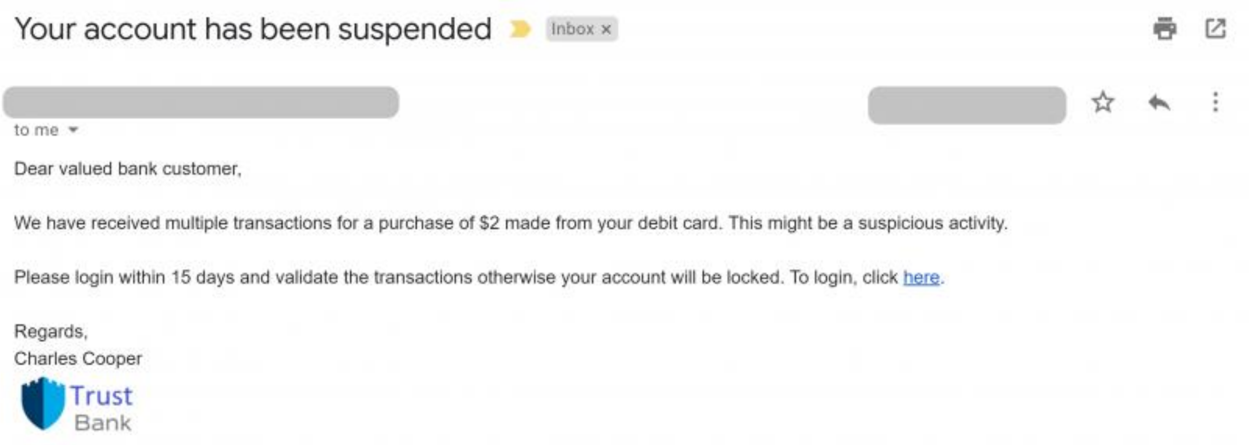
We have received multiple transactions for a purchase of $5,000 made from your debit card. This might be a suspicious activity.

Please login within 15 days and validate the transactions otherwise your account will be locked. To login, click here.

Regards,
Charles Cooper
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

31. Please read the following email to answer the question.



Your account has been suspended

[redacted] [redacted]

to me

Dear valued bank customer,

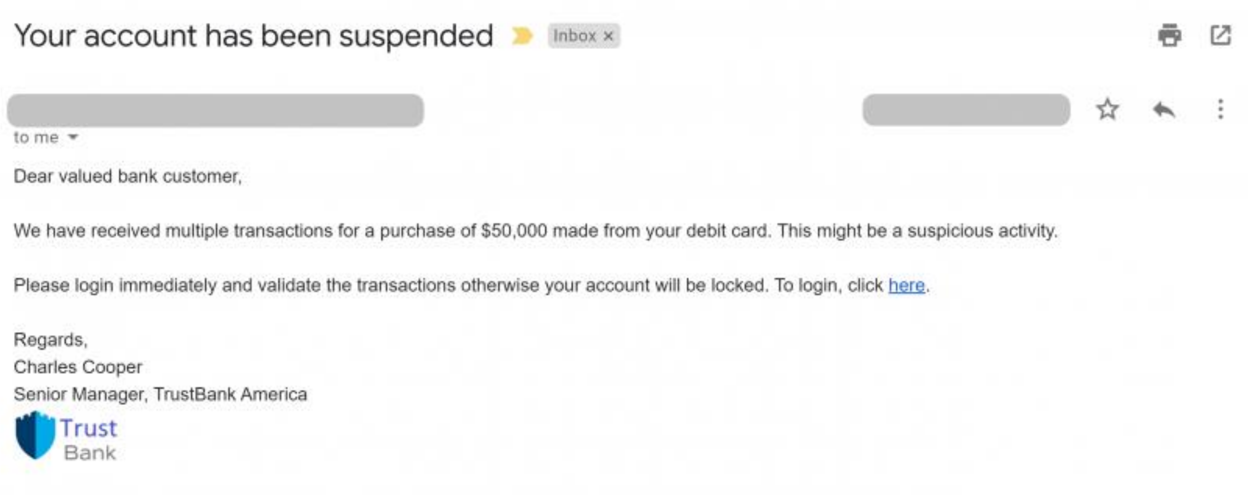
We have received multiple transactions for a purchase of $2 made from your debit card. This might be a suspicious activity.

Please login within 15 days and validate the transactions otherwise your account will be locked. To login, click here.

Regards,
Charles Cooper
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

32. Please read the following email to answer the question.



Your account has been suspended

[redacted]

[redacted]

Dear valued bank customer,

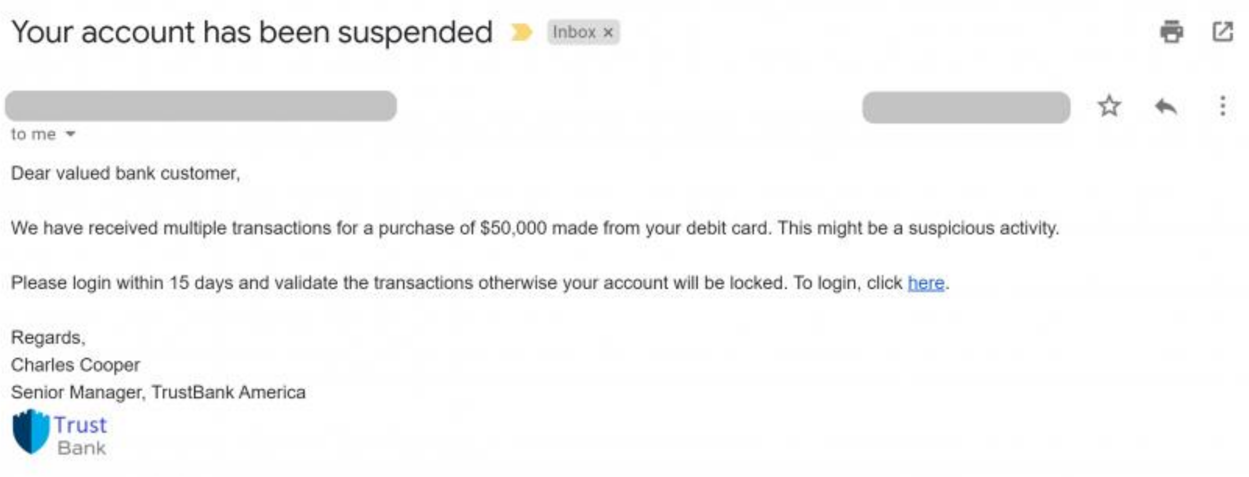
We have received multiple transactions for a purchase of $50,000 made from your debit card. This might be a suspicious activity.

Please login immediately and validate the transactions otherwise your account will be locked. To login, click here.

Regards,
Charles Cooper
Senior Manager, TrustBank America

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

33. Please read the following email to answer the question.



Your account has been suspended

[redacted] [redacted]

Dear valued bank customer,

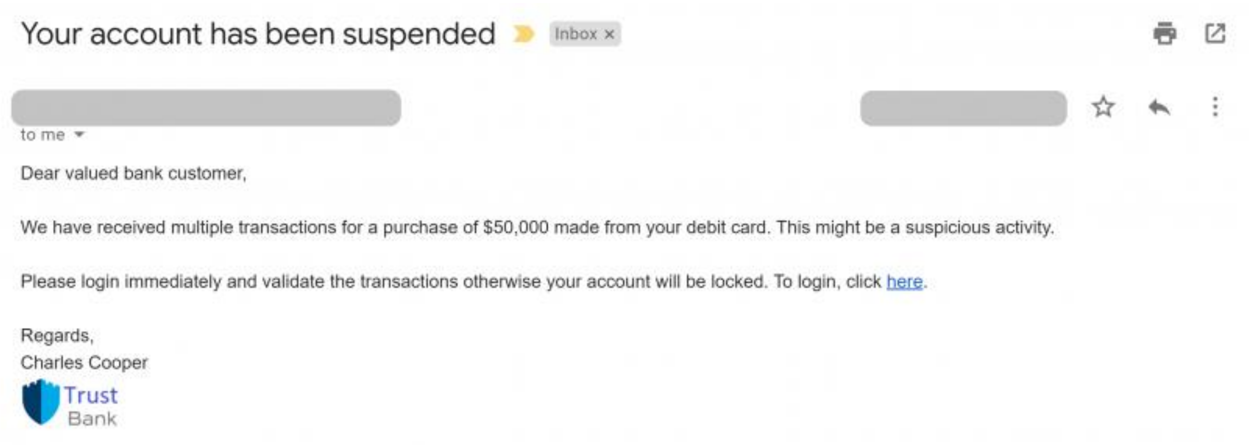
We have received multiple transactions for a purchase of $50,000 made from your debit card. This might be a suspicious activity.

Please login within 15 days and validate the transactions otherwise your account will be locked. To login, click here.

Regards,
Charles Cooper
Senior Manager, TrustBank America
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

34. Please read the following email to answer the question.



Your account has been suspended

[redacted] [redacted]

Dear valued bank customer,

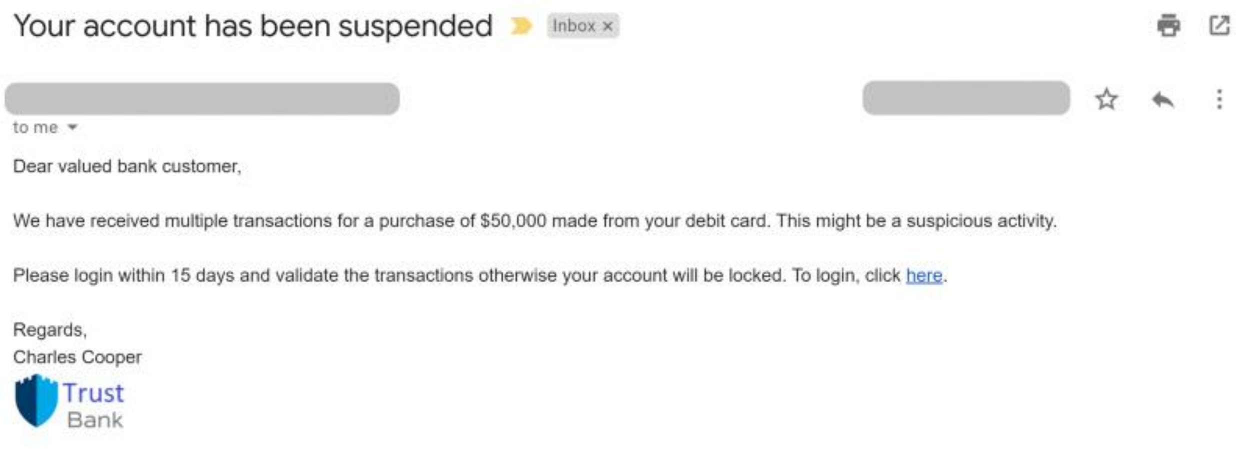
We have received multiple transactions for a purchase of $50,000 made from your debit card. This might be a suspicious activity.

Please login immediately and validate the transactions otherwise your account will be locked. To login, click here.

Regards,
Charles Cooper
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

35. Please read the following email to answer the question.



Your account has been suspended

[redacted] [redacted]

to me

Dear valued bank customer,

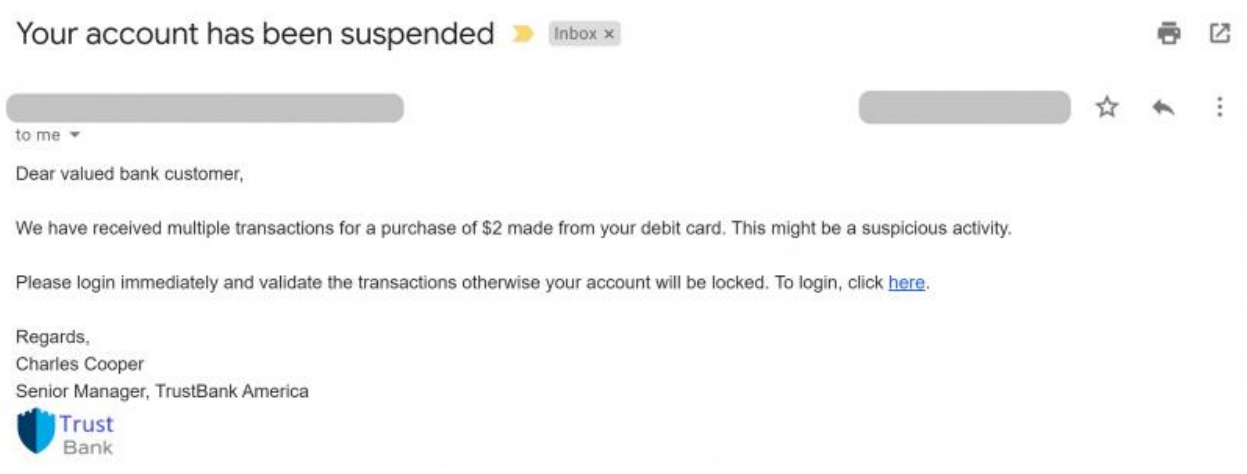
We have received multiple transactions for a purchase of $50,000 made from your debit card. This might be a suspicious activity.

Please login within 15 days and validate the transactions otherwise your account will be locked. To login, click here.

Regards,
Charles Cooper
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

36. Please read the following email to answer the question.



Your account has been suspended

[redacted] [redacted]

to me

Dear valued bank customer,

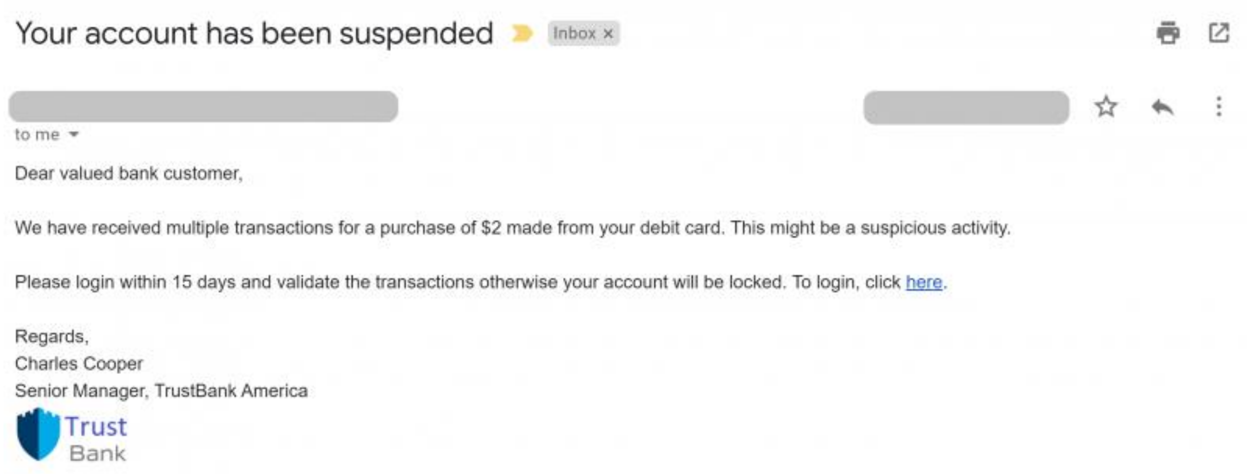
We have received multiple transactions for a purchase of $2 made from your debit card. This might be a suspicious activity.

Please login immediately and validate the transactions otherwise your account will be locked. To login, click here.

Regards,
Charles Cooper
Senior Manager, TrustBank America
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

37. Please read the following email to answer the question.



Your account has been suspended

[redacted] [redacted]

to me

Dear valued bank customer,

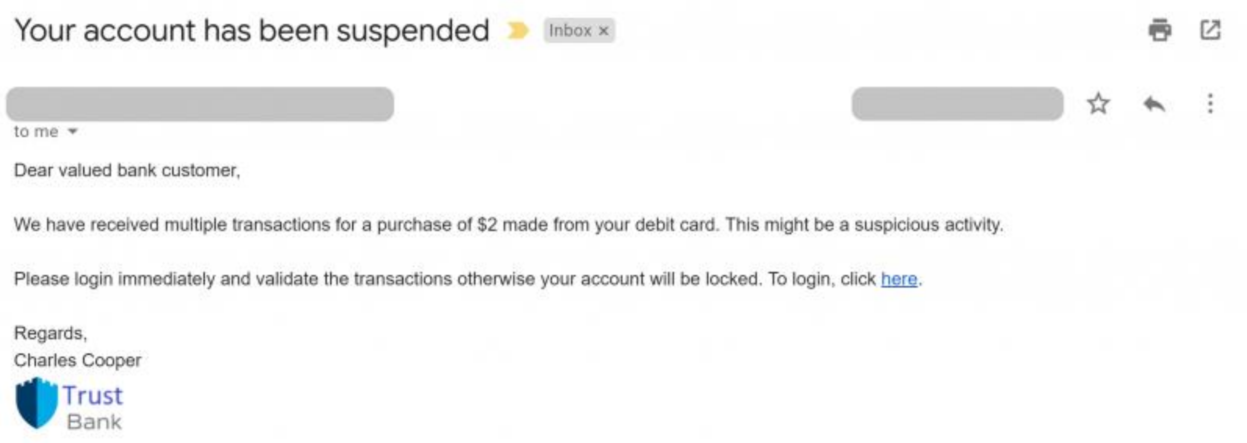
We have received multiple transactions for a purchase of $2 made from your debit card. This might be a suspicious activity.

Please login within 15 days and validate the transactions otherwise your account will be locked. To login, click here.

Regards,
Charles Cooper
Senior Manager, TrustBank America
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

38. Please read the following email to answer the question.



Your account has been suspended

[redacted]

[redacted]

to me

Dear valued bank customer,

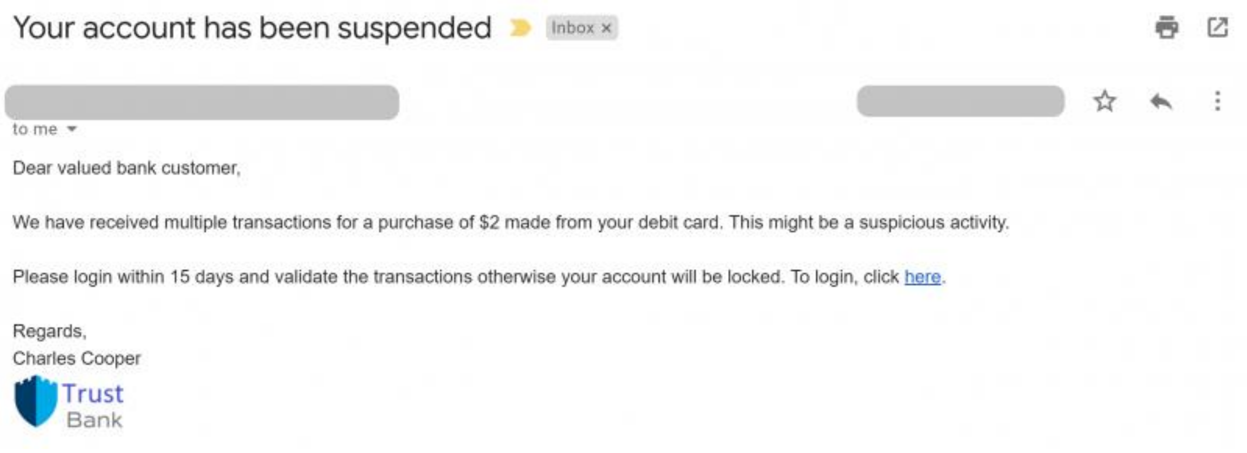
We have received multiple transactions for a purchase of $2 made from your debit card. This might be a suspicious activity.

Please login immediately and validate the transactions otherwise your account will be locked. To login, click here.

Regards,
Charles Cooper
Trust
Bank

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

39. Please read the following email to answer the question.



Your account has been suspended

[redacted]

[redacted]

to me

Dear valued bank customer,

We have received multiple transactions for a purchase of $2 made from your debit card. This might be a suspicious activity.

Please login within 15 days and validate the transactions otherwise your account will be locked. To login, click here.

Regards,
Charles Cooper

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely
How likely are you to click on the link?	□	□	□	□	□

APPENDIX B: RESEARCH PARTICIPANT INFORMATION SHEET

Risk Perception and Human Factors in phishing

Dr. Ida Ngambeki, Priyanka Tiwari
Department of Computer and Information Technology
Purdue University

Key Information

Please take time to review this information carefully. This is a research study. Your participation in this study is voluntary which means that you may choose not to participate at any time without penalty or loss of benefits to which you are otherwise entitled. You may email the researchers to ask questions about the study whenever you would like. If you decide to take part in the study, you will indicate your consent by completing the survey, be sure you understand what you will do and any possible risks or benefits. The purpose of this study is to examine risk perception, and personality traits affecting susceptibility to phishing. This study will take you 15 minutes to 30 minutes to complete.

What is the purpose of this study?

The purpose of this study is to investigate how people of certain personalities are influenced by risk, urgency and authority. You are being asked to participate because you are part of a population for which knowledge and understanding of personal data is important. We would like to enroll 300 people in this study.

What will I do if I choose to be in this study?

If you choose to be in this study, you will receive a link to the survey. The survey will ask questions about risk perception, and personality. Then you will be asked to classify a series of emails as likely or not to be phishing. The survey will be done through Amazon Mturk.

How long will I be in the study?

This study will take you 15 minutes to 30 minutes to complete.

What are the possible risks or discomforts?

Breach of confidentiality is always a risk with data, but we will take precautions to minimize this risk as described in the confidentiality section. Amazon MTurk can potentially be linked to information available on your Amazon public profile page through the Worker ID that the researchers' access. You can choose what is available on your Amazon public profile settings using their settings. We will only be collecting the answers you provide and will not be accessing other information about you that may be part of your Amazon public profile.

This survey has few 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.

Are there any potential benefits?

As a result of this study, you may learn more about your personality, how you perceive risk, urgency factors and authority. This research has the benefit to society of potentially improving general knowledge about authority, perceived risk and personality factors used in phishing.

Will I receive payment or other incentive?

For participating in this study, you will receive $1 as payment on successful completion of the survey.

Will information about me and my participation be kept confidential?

We take participant confidentiality very seriously. The survey does not ask for names, only demographic information. Data will be stored on a password protected file that can only accessed by the researchers. Data will be kept for the duration of the project and archived indefinitely afterwards on PURR. Data will not be used for purposes other than the research questions related to this study.

What are my rights if I take part in this study?

You do not have to participate in this research project. If you agree to participate, you may withdraw your participation at any time without penalty. Once you leave the data collection, we will be unable to identify your data to remove it from the study.

Who can I contact if I have questions about the study?

If you have questions, comments or concerns about this research project, you can talk to one of the researchers. Please contact Ida Ngambeki at 765-496-6839 or ingambek@purdue.edu, Priyanka Tiwari at 765-409-7508 or tiwarip@purdue.edu. To report anonymously via Purdue's Hotline see www.purdue.edu/hotline

If you have questions about your rights while taking part in the study or have concerns about the treatment of research participants, please call the Human Research Protection Program at (765) 494-5942, email (irb@purdue.edu) or write to:
Human Research Protection Program - Purdue University
Ernest C. Young Hall, Room 1032
155 S. Grant St.
West Lafayette, IN 47907-2114

Documentation of Informed Consent

I have had the opportunity to read this consent form and have had the research study explained to me. I have had the opportunity to ask questions about the research project and my questions have been answered. I am prepared to participate in the research project described above. By proceeding with the survey, I am agreeing to these terms.