Journal of the Association for Information Systems

Research Paper ISSN: 1536-9323

Got Phished? Internet Security and Human Vulnerability

Sanjay Goel

University at Albany, SUNY – Information Technology Management, USA
goel@albany.edu

Kevin Williams

University at Albany, SUNY – Psychology, USA
kjwilliams@albany.edu

Ersin Dincelli

University at Albany, SUNY – Informatics, USA
edincelli@albany.edu

Abstract:

A leading cause of security breaches is a basic human vulnerability: our susceptibility to deception. Hackers exploit this vulnerability by sending phishing emails that induce users to click on malicious links that then download malware or trick the victim into revealing personal confidential information to the hacker. Past research has focused on human susceptibility to generic phishing emails or individually targeted spear-phishing emails. This study addresses how contextualization of phishing emails for targeted groups impacts their susceptibility to phishing. We manipulated the framing and content of email messages and tested the effects on users' susceptibility to phishing. We constructed phishing emails to elicit either the fear of losing something valuable (e.g., course registrations, tuition assistance) or the anticipation of gaining something desirable (e.g., iPad, gift card, social networks). We designed the emails' context to manipulate human psychological weaknesses such as greed, social needs, and so on. We sent fictitious (benign) emails to 7,225 undergraduate students and recorded their responses. Results revealed that contextualizing messages to appeal to recipients' psychological weaknesses increased their susceptibility to phishing. The fear of losing or anticipation of gaining something valuable increased susceptibility to deception and vulnerability to phishing. The results of our study provide important contributions to information security research, including a theoretical framework based on the heuristic-systematic processing model to study the susceptibility of users to deception. We demonstrate through our experiment that several situational factors do, in fact, alter the effectiveness of phishing attempts.

Keywords: Phishing, Information Security, Social Engineering, Behavioral Security, Heuristic-Systematic Processing Model, Deception, Cognitive Biases, Vulnerabilities, Security Risk, Threats.

Mikko Siponen was the accepting senior editor. This article was submitted on June 2, 2014 and went through three revisions.

1 Introduction

Social engineering attacks, largely orchestrated through phishing messages, remain a persistent threat that allows hackers to circumvent security controls (Aaron & Rasmussen, 2015). One can manipulate people into revealing confidential information by exploiting their habits, motives, and cognitive biases (Mitnick & Simon, 2002). Countering these characteristics to prevent users from succumbing to phishing emails remains an important research problem that will have a strong impact on information security.

Early research on phishing focused on users' ability to detect structural and physical cues in malicious emails, such as spelling mistakes and differences between the displayed URL and the URL embedded in the HTML code (Jakobsson & Ratkiewicz, 2006). More recent work has focused on cognitive limitations that prevent users from distinguishing between fraudulent and legitimate messages (Dhamija, Tygar, & Hearst, 2006; Downs, Holbrook, & Cranor, 2006). People often process email messages quickly by using mental models or heuristics and, hence, overlook cues that indicate deception (Luo, Zhang, Burd, & Seazzu, 2013). In addition, people's habits, needs, and desires make them vulnerable to phishing scams (Workman, 2007). Watters (2009) concludes that phishing messages elicit automatic modes of response based on structural cues rather than careful deliberation using cognitive processing. If the message suggests it will fulfill, or threaten, important needs, the reader may overlook cues that indicate deception.

Awareness of phishing messages among users has increased, but so has the sophistication of these messages (Jagatic, Johnson, Jacobsson, & Menczer, 2007). Hackers design phishing messages today to affect basic human emotions (e.g., fear, greed, and altruism) and often target specific groups to exploit their specific needs. Hackers sometimes even contextualize the messages to individuals by incorporating their personal information (spear phishing). For instance, a new phishing scam has arisen on dating applications; a user (bot) triggers a conversation with another user (victim) and, after a few exchanges, sends a link (malicious) to the victim ostensibly with a picture in an attempt to get the victim to click on it (Jones, 2015). Research shows that spear phishing is more effective than broad phishing messages, which target a wider population (e.g., Wang, Herath, Chen, Vishwanath & Rao, 2012), but few, if any, studies have compared the relative effectiveness of messages contextualized to elicit different emotions in users. We designed our study to fill this gap in the literature.

In this paper, we consider different cognitive biases that inveigle users to click on phishing messages. We focus on the content and framing of these messages and identify the types of messages most likely to deceive users. Specifically, we examine the effectiveness of different contextualized messages designed to exploit basic human emotions and desires. Research in cognitive neuroscience shows that emotions play an important role in decision making by subconsciously steering people toward gains and away from losses (Damasio, 1994). A carefully constructed phishing email may activate basic emotions that nudge people to comply with the disguised malicious request. For example, fear stems from the perception of threat to one's wellbeing and acts as a warning signal for forthcoming harm (LeDoux, 2003). Fear increases immediate precautionary action to protect oneself and one's possessions (Leventhal, 1970). A typical banking scam exploits fear reactions by suggesting that users will have their account blocked unless they change their credentials by clicking on a Web link. The fear of losing something valuable might result in users divulging their credentials to the hacker (Kim & Kim, 2013). Greed is another emotion that hackers who craft phishing emails often exploit (Hong, 2012). The infamous "Nigerian Prince" scam capitalizes on the allure of easy money to deceive and cheat its victims. Coupling greed with scarcity, such as "only a few laptops left" or "the first two hundred respondents are eligible", may establish a sense of urgency (or a fear of losing out) that increases the perceived value of the object (Cialdini, 1993) and may can cloud rational judgment even more (Hong, 2012).

Of course, phishing attacks can manipulate many other emotions and related psychological traits, such as curiosity, anger, patriotism, friendship, altruism, vanity, authority, community belongingness, and sense of duty. In this study, we examine how the framing of message content affects susceptibility to phishing attempts. We manipulate fraudulent email messages to appeal to different desires or needs and contextualize the messages by framing them as either potential gains or losses. We tested the effectiveness of the different messages in a naturalistic setting using college students. The research design also allowed us to examine differences in susceptibility among different subgroups (e.g., males vs. females; academic major).

This paper proceeds as follows: in Section 2, we discuss the extant literature. In Section 3, we discuss the theoretical basis for our research and our hypotheses. In Section 4, we present the research design and review the experimental methodology. In Section 5, we present the experimental results. In Section 6, we discuss the results in detail and present the study's implications and limitations. Finally, in Section 7, we conclude the paper.

2 Literature Review

Phishing's foundations lie in human decision making where one persuades someone else to make non-rational instinctive and emotional choices rather than more deliberative and logical choices—in this case, on clicking malicious links. Anderson and Moore (2009) emphasize that heuristics and biases drive decision making, especially when the user is emotionally aroused and in unusual conditions. The research on phishing correspondingly focuses on understanding the triggers for non-rational decisions and aims to steer users towards more deliberative and rational choices. A large fraction of phishing research involves testing users' susceptibility to phishing when faced with different scenarios and evaluating the impact of interventions on reducing this susceptibility as we discuss further in the literature review. One can broadly classify phishing research into two categories: 1) susceptibility to phishing, including psychological factors, individual differences (e.g., cognitive limitations, personality traits, identity, and demographics), and structural features of the messages (e.g., presence of misspelling); and 2) solutions to reduce susceptibility to phishing (e.g., toolbars and training). Subsequently, we summarize the literature and lay out the motivation for our research in the following subsections.

2.1 Susceptibility to Phishing

Psychological factors are at the core of human vulnerability to deception, and some exploratory work has focused on ascertaining these factors as they relate to phishing. The factors that this research has examined include cognitive limitations, familiarity, emotional arousal, social psychological factors (e.g., trust, fear, and commitment), personal relationships, personality traits (e.g., neuroticism, extroversion, and openness), and demographic variables. We discuss this research in three segments (i.e., psychological triggers, individual differences, and visual/structural cues).

2.1.1 Psychological Triggers for Phishing

Extant literature has attributed phishing susceptibility to human cognitive limitations and psychological manipulation of victims as we discuss further in this section. Dhamija et al. (2006) discuss human cognitive limitations in being able to detect fraudulent messages. They identify five broad categories of strategies that users employ to identify fraudulent websites based on content, URL analysis, URL protocol (i.e., https), and other visual security cues such as use of HTTPs, bar padlocks, and security certificates. All of the subjects in the study performed at a 40 percent error rate, and the authors found no statistically significant difference between the methods the participants used to identify fraudulent websites.

Downs et al. (2006) investigated the impact of risk familiarity in informing phishing defense strategies. They provided fake identities to twenty subjects and asked them to roleplay email and Web interactions. They found that, when users were exposed to specific scams and could comprehend their modalities, they could protect themselves. However, participants could not defend themselves when exposed to deception that was sophisticated or novel. These results suggest that heuristics that many increase one's susceptibility to phishing scams guide individuals' responses to email requests (e.g., "Amazon is a reputable company, and I may have already given them the information they are asking for; therefore, I would be comfortable giving the information to them again.").

Workman (2008) investigated whether the factors that result in successful marketing campaigns also affect the success of social engineering attacks such as phishing and pretexting. He reviewed the literature on security, management, and social psychology and highlighted important factors that may impact the success of social engineering attacks: trust, fear, commitment, and reactance. He examined the relation between these factors and employee susceptibility to social engineering attacks and found a strong positive correlation of social engineering with trust, fear, and commitment—both for self-reported and observed behavior.

Some work has focused specifically on spear-phishing attacks; that is, phishing emails customized to a specific individual or organization rather than to a specific demographic (students, elderly, women, etc.) or the general population at large. Jagatic et al. (2007) examined whether email senders' personal relationships altered the recipient's susceptibility to phishing attacks. They sent (benign) phishing messages to university students that appeared to come from friends of the subjects using data mined from their profiles online social networks. The manipulated messages produced an 80 percent susceptibility rate compared to only 16 percent for the control group, suggesting that people are more likely to be deceived if messages appear to come from someone in their social network. The study identified the gender of the user (recipient) from their Facebook profile and found that the sender's gender did not have an independent effect on susceptibility. Halevi, Lewis, and Nov (2015) found that 25 of 40 employees (62.5%) clicked on a link embedded in a fraudulent email purportedly from the company's IT manager and addressed to them individually. Egelman, Cranor, and Hong (2008) tested the effectiveness of security warnings by simulating spear-phishing attacks that exposed users to such warnings. They found out that the participants were susceptible to spear-phishing emails and that active phishing warnings demonstrated greater protection against spear phishing.

Butavicius, Parsons, Pattinson, and McCormac (2015) conducted a phishing experiment to examine how phishing messages created using three social engineering strategies (authority, scarcity, and social proof) influenced users' judgments of how safe a link is in an email. Their experiment included genuine, phishing, or spear-phishing messages. They found that content based on authority was the most effective strategy in convincing users that the link was safe while social proof was the least effective. Also, 71 percent of participants had difficulty distinguishing between genuine and spear-phishing emails and fell prey to phishing emails. Wright, Jensen, Thatcher, Dinger, and Marett (2014) used principles of persuasion to design emails and test their efficacy in phishing susceptibility. They found that messages designed with principles of persuasion were more effective; however, the efficacy of different principles varied.

2.1.2 Individual Differences in Susceptibility to Phishing

Different individuals have a different propensity to becoming victims of phishing attacks based on behavioral traits, demographic characteristics, personality, and habituation; we discuss these individual differences in this section. Moody, Galletta, Walker, and Dunn (2011) extensively investigated individual differences in susceptibility to phishing. They examined disposition to trust and distrust, curiosity, entertainment drive, boredom proneness, lack of focus, risk propensity, and level of Internet usage, attachment to the Internet, and Internet anxiety as the traits related to susceptibility. They found that several of the traits were good indicators of susceptibility to phishing, most notably trust, curiosity, boredom proneness, and risk propensity.

Sheng, Holbrook, Kumaraguru, Cranor, and Downs (2010) focused on demographic characteristics (gender, age, and education level) as predictors of phishing susceptibility. They found that women were more susceptible to phishing than men and that the 18- to 25-year-old individuals formed the most susceptible age group. Flores, Holm, Nohlberg, and Ekstedt (2015) examined cultural differences and personal determinants (e.g., intention to resist social engineering, security awareness, and training) of phishing. In contrast to Sheng et al. (2010), they did not find a significant correlation between phishing behavior and age or gender in their study. They found significant positive correlations between employees' observed phishing behavior and intention, security awareness, and training; however, the strength of correlations differed across different cultures (i.e., US, India, and Sweden). Correlations of both intention and security awareness to phishing behavior were not significant for American and Indian individuals but were for Swedish individuals. The correlation between training and phishing behavior was stronger for the American individuals compared to Swedish individuals and non-significant for Indian individuals.

Halevi, Lewis, and Memon (2013) used the five-factor model of personality to examine the relation between personality and vulnerability to phishing. The five behavior traits in this model are neuroticism, extroversion, openness, agreeableness, and conscientiousness. The authors sent a sample of 100 college students (83% male; ages 17-21) (benign) phishing emails with a malicious link. Specifically, they sent the sample an email that promised a prize of an Apple product to test the individuals' susceptibility to phishing, and the authors considered that they had phished the participants if they clicked on the embedded link. Results showed that females were significantly more likely to be "phished" than men and that students high in neuroticism were more susceptible to the phishing attacks. While interesting, the research does not delve into the psychological reasons of the susceptibility or compare different motivators in susceptibility to phishing.

Vishwanath (2015) investigated the role of habit and cognitive processing in victimization to phishing. He sent 200 randomly selected students a phishing email with an attached survey. He obtained measures of the subjects' level of heuristic and systematic processing, information sufficiency, and personality traits. He hypothesized that systematic (as opposed to heuristic) processing of data would result in lower incidence of phishing victimization. He found that students with low emotional stability had impulsive email habits such as reactively checking email and responding to email notifications and were more likely to click on phishing email links. We elaborate further on systematic and heuristic processing in our theoretical development in Section 3.

2.1.3 Physical Attributes of Messages in Susceptibility to Phishing

Some research has investigated the impact of phishing emails' physical features on users' susceptibility to phishing. For instance, Jakobsson and Ratkiewicz (2006) sent phishing emails with links crafted to look suspicious (e.g., spelling mistakes, escape characters, and naked IP addresses in the URL) and found that four to 14 percent of users still clicked on those links. In a different study, Jakobsson, Tsow, Shah, Blevis, and Lim (2007) examined the effectiveness of trust indicators in email and webpages wherein they asked users to identify features that provoked trust. Their findings indicated that 1) sophisticated layout and legal disclaimers engender trust (e.g., copyright notices), 2) too much emphasis on security is counterproductive, 3) individuals use URLs extensively to evaluate trust, and 4) the impact of third party endorsement varies by whether one recognizes the party's name.

Wang et al. (2012) studied how users process visual cues and detection indicators of phishing messages and decision making process. They found that attention to visceral triggers and phishing detection indicators and to users' phishing knowledge played a critical role in phishing detection. Harrison, Vishwanath, Ng, and Rao (2015) found that information that alludes to social presence fosters heuristic decision making and increases susceptibility to phishing. The authors manipulated social presence with cues such as the university logo, versing security logo, and click-to-chat icons.

2.2 Countering Phishing Messages

Some research has examined the impact of training users in recognizing features in phishing messages to reduce susceptibility to phishing; however, most research has primarily focused on susceptibility to phishing. We have some evidence that educating individuals about common phishing practices reduces their likelihood of being phished (Kumaraguru, Cranor, & Mather, 2009a; Kumaraguru et al., 2009b; Sheng et al., 2010); however, results regarding the efficacy of training have been generally disappointing (Görling, 2006). Anandpara, Dingman, Jakobsson, Liu, and Roinestad (2007) contend that training individuals with phishing IQ tests is ineffective at improving susceptibility because it simply raises fears related to phishing rather than making users better at discerning whether an email is phishing them or not. Still others believe that the effects of such training are short term (Caputo, Pfleeger, Freeman, & Johnson, 2014). There are, however, innovative ways in which one can make phishing education effective. Kumaraguru et al. (2007) and Sheng et al. (2007) demonstrate the use of innovative learning designs based on learning science principles for anti-phishing education. Mayhorn and Nyeste (2012) show that training through comic strips and video games is very effective at reducing vulnerability to social engineering. Arachchilage and Love (2013) show that a game design framework for avoiding phishing attacks is very effective.

In addition to training, researchers have developed other various anti-phishing solutions to reduce individuals' susceptibility to phishing attacks (Emigh, 2005), such as toolbars, browser add-ons, and indicators (e.g., Netcraft and Web of Trust). Dhamija and Tygar (2005) propose an authentication scheme named Dynamic Security Skins that allows users to distinguish "spoofed" webpages using a unique image for each transaction. The scheme displays the image as a "skin" on the transaction window so that the user can verify that the images match and authenticate the content generated by the server. Wu, Miller, and Garfinkel (2006) evaluate the effectiveness of security toolbars as a deterrent to phishing. They conducted a study in which they required participants to respond to twenty emails, five of which were phishing manipulations. They found 33-45 percent incidence of clicking on phishing emails when toolbars were allowed. They also found that providing pop-up blocking warnings reduced the rates, but 70 percent of participants still succumbed to at least one deceptive email.

2.3 Summary of Prior Research

As we can see, the research suggests that psychological factors such as trust, fear, and obedience to authority may increase susceptibility to phishing. Most published studies have focused on users' susceptibility to generic phishing messages without contextualization. Contextualizing messages may increase the effectiveness of phishing, which the recent studies on spear phishing evidence. However, one may not need to personalize phishing messages to be effective; messages designed for a particular group of people may be effective if they identify group-relevant concerns and elicit specific emotions that trigger the desired response. To date, few studies have experimentally investigated the effects of contextualization or directly compared different contextualized messages. As such, we test the effectiveness of contextualized messages designed to elicit different emotions in a targeted population (students). We also adopt a theoretical framework that explains how contextualized messages may increase users' susceptibility to phishing by causing them to make hasty judgments based on initial impressions of the immediate context but also stand up to scrutiny should the users consider the message more carefully.

3 Theoretical Foundations

The considerable research attention that has focused on phishing susceptibility lately lacks an integrating theory. We draw on theories from social and cognitive psychology to provide the conceptual framework for our research. Our basic premise is that successful phishing attacks take advantage of the human tendency to make quick and intuitive judgments based on initial impressions of the immediate context. Although phishing messages contain false information that one may detect with careful scrutiny or investigation, a well-crafted message activates specific motives that push victims toward accepting the message.

Contemporary theories of information processing propose that two modes of processing exist: one quick and intuitive and one slow and deliberate. For example, Kahneman (2011) distinguishes between 1) an automatic and quick mode of thinking designed to detect simple relationships and to integrate information to maintain and update perceptions of our world (system 1) and 2) a slower, deliberate mode of thinking associated with the subjective experiences of agency, choice, and concentration (system 2). Whereas system 1 is a "machine for jumping to conclusions", system 2 allocates attention to effortful mental activities and can compare objects on several attributes, follow rules, and make choices. Similarly, Petty and Cacciopo's (1986) elaboration likelihood model (ELM) of persuasion identifies two cognitive processing routes to persuasion: a central and a peripheral path. The peripheral path is characterized by limited conscious attention that relies on cues and mental shortcuts that bypass counter-argumentation, whereas the central route relies on rational analysis that involves elaborating on information and arguments. When processing information peripherally, people do not think carefully about the content of the message; instead, they are influenced by superficial factors surrounding the communication. Phishing attempts often capitalize on peripheral routes to persuasion by incorporating cues that provoke action without careful deliberation. Such superficial features that often produce action are cues related to authority, scarcity or urgency, reciprocity, and similarity. In a phishing context, individuals will likely process emails from purported authority figures (e.g., bank officials and school administrators) that stress urgent action or evoke feelings of reciprocity along the peripheral path and, thus, lead to action without the user's carefully considering the request. Both Kahneman's theory and Petty and Cacciopo's ELM predict that successful phishing attempts work by pushing or nudging users to divulge information without provoking excessive thought.

Although quickly or peripherally processing information may increase the likelihood of deception, it does not sufficiently explain victimization. One cannot describe people victimized by the Nigerian Prince scam, for example, as always operating in a peripheral or quick thinking mode. Rather, the two modes of processing may occur simultaneously, and some successful phishing attempts capitalize on both systems. The heuristic-systematic processing model (HSM) (Chaiken, 1987; Chen & Chaiken, 1999) provides a strong conceptual basis for understanding how this processing may occur. According to HSM, people use a combination of heuristic (quick) and systematic (deliberate) processing modes to reach judgments. Heuristic processing refers to relying on judgmental rules and cognitive shortcuts (heuristics). It is associated with rapid decisions that individuals often base on immediate emotion and is subject to cognitive biases. Systematic processing involves carefully scrutinizing information and refers to analytically and comprehensively dealing with messages. HSM invokes the principle of least effort; that is, people tend to choose the course of action that requires the least effort, and, thus, heuristic processing often takes precedence over more effortful systematic processing (Eagly & Chaiken, 1993). But heuristic processing does not mean that people ignore motivational concerns. Rather, people sense motivational concerns in the immediate context and then try to spend minimal cognitive effort meeting those immediate motivational concerns. A critical concept in HSM is the notion of a sufficiency threshold, which refers to a desired level of confidence that people have for their judgments (Eagly & Chaiken, 1993). Confidence in one's decision or judgment must pass this threshold level; according to HSM, people will continue processing the message until they are confident that they have surpassed the sufficiency threshold. If people can reach the sufficiency threshold with heuristic processing, then they stop processing information. Otherwise, they are likely to use systematic processing until they reach the sufficiency threshold. The HSM also proposes that one can adjust the sufficiency threshold up or down depending on contextual factors, such as how important the decision is, or how much time pressure one is under. When pressed to make a decision quickly, for example, people may lower their sufficiency threshold, which makes it easier to reach with heuristic processing alone.

Luo et al. (2013) applied HSM to phishing attacks to outline the anatomy of a successful attack. They argue that successful phishing attacks increase individuals' heuristic processing and suppress their systematic processing. Attackers can do so by luring recipients to quickly but inaccurately assess the validity of the message or by reducing the sufficiency threshold so that recipients do not initiate systematic processing. If, however, the recipient fails to remain in heuristic processing mode, the successful (phishing) message is also one built to "withstand" systematic processing, such that, even if recipients scrutinize the message more carefully, they still make an inaccurate assessment of its validity. As Luo et al. (2013) summarize, heuristic and systematic processing may produce the same conclusion and, thereby, increase one's confidence in the judgment. Heuristic processing may create an initial impression that systematic processing subsequently confirms (i.e., a confirmation bias; Kahneman, 2011).

Luo et al.'s (2013) framework suggests that research should focus on factors that: 1) increase the likelihood that recipients will rely on heuristic processing; 2) lower the sufficiency threshold; and/or 3) increase the chances that a message will stand up to scrutiny. We argue that contextualizing an email message to quickly trigger motivational concerns in a context that appears specific to the recipient lowers the sufficiency threshold and helps the message withstand scrutiny should heuristic processing give way to more systematic processing. For example, course registrations are important to college students, and a message that threatens their continuance is likely to create a sense of urgency and the need for quick action. A strong emotion such as fear of losing something of value may subconsciously predispose or push people toward action (Damasio, 1994). As a result, students may quickly respond to a request for personal information in order to secure their courses. In this sense, contextualization acts like pretexting in social engineering attacks. In pretexting, one invents a scenario and incorporates something of specific relevance or importance to the recipient in the scenario, which acts to legitimize the interaction and can induce the recipient to divulge information (Anderson, 2010; Luo et al., 2013). One can also see contextualization as a form of spear phishing, where the attacker targets specific individuals with personalized messages. Typically, spear-phishing victims receive an email that appears to be from someone they know, which increases their trust in the message. In both pretexting and spear phishing, a carefully manipulated context underscores the importance of immediate action, which may simultaneously encourage heuristic processing, increase trust, and lower the sufficiency threshold and, thereby, obviate the need for careful scrutiny of the message.

H1: Contextualized email messages that relate to a recipient's specific concerns increase susceptibility to phishing compared to non-contextualized emails that relate to general or broad concerns.

Another factor that is likely to influence the sufficiency threshold and susceptibility to deception is whether the message is framed to suggest that the recipient gains or loses something of value. People are motivated to gain things of value, and they may be induced to divulge personal information with the allure of money or material goods. However, research associated with prospect theory (Kahneman & Tversky, 1979) suggests that potential losses exert a stronger influence over people's judgments and actions than potential gains. Prospect theory is a descriptive theory of decision making under uncertainty that explains when people will be seek or avoid risk. A key principle of prospect theory is that the way in which people frame an outcome affects their actions. Two key concepts influence judgments: reference dependence and loss aversion. Reference dependence refers to the fact that individuals evaluate decision outcomes relative to a reference point, often the status quo. Individuals see outcomes above the reference point as gains and outcomes below the reference point are as losses. People attach subjective values to gains and losses, such that gains are associated with positive value and losses with negative value. People are maximally sensitive to change near the reference point (greater value attached to amount of change from status quo), and individuals weigh losses more heavily than gains. That is, the pain of losing $100 is greater than the joy of gaining $100. Prospect theory has two important implications for phishing. First, a phishing message crafted to induce an immediate sense of change from the status quo (either in terms of gaining something desired, such as a free gift card, or in terms of preventing the loss of something desired, such as money) will more likely deceive people. Second, the threat of an immediate loss is particularly likely to spur people to action. The negative value associated with loss may lower the sensitivity threshold and produce the belief that quick compliance with the email request will prevent the loss. Thus, messages that threaten the loss of something valuable may be more effective than messages offering the possibility of gain.

H2: Phishing messages that frame potential outcomes as losses are more effective than messages that frame outcomes as gains.

The types of motives and emotions elicited in the recipient may also influence a phishing message's effectiveness. Few studies have examined the motives that phishing messages elicit despite Downs et al.'s (2006) finding suggesting that emails' content is more likely to influence the judged trustworthiness of an email than peripheral cues in headers and subject lines. Drawing on work in evolutionary and social psychology, Lawrence and Nohria (2002) identified four broad, universal motivational drives or "emotional needs" in humans: 1) the drive to acquire, 2) the drive to defend, 3) the drive to bond, and 4) the drive to learn. The drive to acquire relates to the motivation to secure scarce goods for oneself, including intangibles such as social status. One can see achievement and power motives, along with emotions of greed and envy, as manifestations of the drive to acquire. The drive to defend refers to the motivation to protect oneself, one's family, and one's possessions against external threats (physical and psychological). Fear of losing something of value triggers the drive to defend. The drive to bond relates to the pervasive drive to form and maintain lasting, positive interpersonal relationships. Humans desire social connections and, thus, are motivated to join and remain in groups. The drive to learn refers to the motivation to satisfy our curiosity and master our environments. Deceptive content that activates one of these basic emotional needs or drives will most likely to deceive recipients and convince them to divulge personal or sensitive information. In this study, we manipulate the content of phishing emails to activate the first three drives; that is, to acquire, to defend, and to connect. Although these drives are universal, the context in which they operate may vary. For example, face-to-face interactions with others may activate, for example, the drive to bond more easily than asynchronous email communications. However, email communications that identify a path or mechanism for obtaining valued tangible or intangible outcomes may more easily activate the drive to acquire. Thus, we might expect that the motive to acquire, along with associated emotions such as greed, will lower the sufficiency threshold and make people more susceptible to phishing.

H3: Phishing messages that offer recipients the opportunity to acquire new outcomes (tangible or intangible) are associated with greater susceptibility than messages associated with social outcomes.

4 Research Design

Finn and Jakobsson (2007) discuss ethical and technical issues regarding phishing experiments. They define three principal approaches that researchers have used to quantify responses to phishing attacks: surveys, closed-lab experiments, and imitation studies. Survey studies require participants to report their own behaviors. One serious drawback of survey studies is that participants are apt to underestimate or overestimate the possible damages of phishing attacks; they may not be aware of the phishing attack or may not be willing to disclose that they have fallen prey to a phishing attack. Closed-lab experiments allow researchers to evaluate phishing attacks and their countermeasures in a controlled environment, but, at the same time, the participants of such experiments might be biased because they are aware that they are part of an experiment. The third strategy uses deception and imitates real phishing attacks to measure the actual success rate of these attacks under realistic (albeit ultimately benign) conditions. Although the imitation approach is the most realistic research strategy, it possesses ethical concerns because mimicking a phishing attack involves deception and, hence, poses risk of psychological harm or negative reactions in participants. We used the imitation strategy to measure actual behaviors as realistically as possible. However, we included an informational page in the follow-up survey that explained the purpose of the study and how phishing works and provided participants advice about how to avoid phishing attempts (Appendix 2).

Phishing involves multiple discrete steps that culminate with the user's revealing confidential information to the hacker. The first step is the deception, whereby the victim receives a phishing email, reads the email, and is motivated to react. The second step involves the user's clicking on the link to the phishing webpage and evaluating the information on the page. The third step involves further deception in that the user is convinced to reveal personal information such as credit card number, social security number, or banking information. The user does not necessarily need to follow through to step 3 for the hacker to breach their security. Step 2, in which a user clicks on the fraudulent link, can result in the user's downloading malware to the user's computer, which can cause damage to the computer or, worse yet, install a backdoor through which the hacker can gain access to it. The key question that we address in this research is: what causes people to be deceived by phishing messages, and what motivates them to click on phishing links?

Specifically, we examine the first and second steps of the phishing process, and then, instead of having users reveal their personal information, we direct participants to a benign website, inform them that they have fallen prey to phishing, provide an educational message, and request that they voluntarily complete a survey that assesses their security perceptions and personality traits.

We designed the emails' content to test the hypothesized effects of gain/loss frame, contextualization, and motive. We used positively and negatively framed messages to portray gains and losses, respectively. Positively framed messages presented recipients with the opportunity to acquire something of value (e.g., gift card, iPad mini, computer virus software, and feelings of altruism). Negatively framed messages threatened recipients with the loss of something of value (course registrations and money in bank accounts) or the loss of a potentially valuable opportunity (opportunity for tuition assistance). We varied contextualization in two ways. First, we varied outcomes so that they pertained specifically to students at the university (e.g., course registrations and tuition assistance) or to any person (e.g., $50 gift card and iPad mini). Second, we portrayed the message sender as being from in the university (e.g., student accounts manager) or external to the university (e.g., the Apple research team). Finally, we intended the messages' content to activate individuals' motives to acquire things, protect assets, or connect to/help others. We created eight messages, four with a "gain" frame and four with a "loss" frame. Table 1 summarizes the eight emails.

Table 1. Characteristics of Phishing Emails

Content	Gain or loss	General motive	Contextualization
Gift Card	Gain	Acquisition	Low
iPad Mini	Gain	Acquisition	Low
Virus & firewall software	Gain	Defense	High
Volunteer	Gain (altruism)	Social	Low
Course registration	Loss	Acquisition	High
Bank card	Loss	Acquisition	High
Tuition assistance	Loss (of opportunity)	Acquisition	High
Alumni social network	Loss (of opportunity)	Social	High

The participants in the study were third- and fourth-year students enrolled at a large research university in Northeastern USA. We used a university setting for this study because students frequently fall victim to similar online threats (Johnston & Warkentin, 2010) and because researchers consider them an appropriate group for such applied behavioral research (Gordon, Slade, & Schmitt, 1986). They also fit in the age bracket most susceptible to phishing. We categorized students into four groups according to their broad academic major: social sciences, STEM (science, technology, engineering and mathematics) fields, humanities, and business. The total dataset included 7,225 students, with 3,513 females and 3,712 males. The breakdown by major was as follows: social sciences: 1,791 females and 1,554 males; business: 340 females and 554 males; humanities: 610 females and 518 males; and STEM: 772 females and 1,086 males.

Working with the information technology services professional staff and with institutional review board approval and oversight, we obtained email addresses for all third- and fourth-year undergraduate students. We divided the student sample based on the four broad academic majors and created male and female subgroups in each category. We then randomized each of the eight subgroups and split them into eight blocks. We gave each block a different treatment (email message) based on the framework we define in Table 1. Our factorial design was four major categories x two genders x eight interventions. Table 2 shows the number of recipients for each of the 64 groups.

Table 2. Breakdown of Recipients Based on Eight Different Phishing Email (7,225 in total)

	Field	Gift card	Tuition assist.	iPad	Registration	Firewall	Bank card	Volunteer	Social network
Female	Social science	224	224	224	224	224	224	223	223
	Business	43	43	43	43	42	42	42	42
	Humanities	77	76	76	77	76	76	76	76
	STEM	97	97	97	97	96	96	96	96
Male	Social science	195	194	195	195	194	194	194	194
	Business	70	69	69	70	69	69	69	69
	Humanities	65	65	65	65	65	65	64	64
	STEM	136	136	136	136	136	136	135	135

We used an automated email distribution service to distribute the phishing emails. The service allowed us to track the emails through the entire phishing process; that is, when users received the email, when they read it, and when they clicked on the phishing link. The service allowed us to create accounts (with arbitrary client addresses) from which we distributed the emails. We created email addresses with the university's "edu" domain extension to imply authenticity and increase the users' trust in the email (i.e., if the user hovered the mouse over the sender's name, it would show an email with "albany.edu" extension, such as itm_maillist1@albany.edu). This technique mimics sophisticated phishing strategies currently in use. To comply with the service's usage policy, we added an unsubscribe message to the bottom of the email, which constituted a single line of text with a link to the email address of the account from which the email was sent. Each email contained a fake phishing link, which was actually a link to the participant survey. Each link uniquely corresponded to a different email so that we could aggregate the responses to specific email accounts. We masked the survey links using a different service to hide the true identity of the link. To make the links more convincing, we used a link that included both the word "ualbany" and a word related to the specific phishing email (e.g., "giftcardsurvey") (e.g., http://ualbany.9nl.com/giftcardsurvey/).

We considered the timing for the experiment carefully because we needed to choose a time that students would most likely check and read their emails. We collected data for 15 days, starting from the last week of classes to end of final examinations to make sure that most of the students saw the emails (Ferguson, 2005). We tracked the number of recipients who opened the phishing emails and the number of users out of the ones who opened the email who actually clicked on the phishing link embedded in the email. Once a user clicked the phishing link, the link directed the user to the survey website. This website contained an informational page that informed the user of the phishing experiment and provided tips for good practices to avoid phishing (Appendix 2).

4.1 Participant Survey

Via the survey website, we asked participants who clicked on the link to complete a survey at the end of the informational message to obtain data on users' perceptions and individual differences. Only a small fraction of students actually completed the survey, so we treated these data as exploratory. The survey questionnaire assessed users' computer security, their perceptions and scrutiny of the email, and personality traits. We asked participants whether they had a firewall and/or a virus protection program running on their computer (response options were "yes", "no", and "I don't know"). We also asked them how many times their computer had been infected with a virus or malware in the past. Four questions assessed security and anti-phishing behaviors related to the phishing email. We asked participants if they scrolled over the link in the email before clicking on it and whether they searched for information on the topic before responding (response options were "yes" and "no"). We also asked them how suspicious they were of the email on a four-point Likert scale (1 = not at all suspicious, 2 = a little suspicious, 3 = fairly suspicious, 4 = very suspicious). We also asked them if they read the email carefully on a four-point Likert scale (1 = not very carefully at all, 2 = somewhat carefully, 3 = carefully, 4 = very carefully). We measured the personality traits conscientiousness, neuroticism (emotional stability), extraversion, ambition, and achievement drive using a self-report, commercial personality inventory. We assessed the reliability for these scales using Cronbach's alpha and found them to be acceptable for each scale: .79 for conscientiousness, .96 for extraversion, .91 for neuroticism, .72 for ambition, and .73 for achievement drive.

5 Results

A total of 7,225 phishing emails were sent to students and registered as received. Records showed that 1,975 students opened the email that they received, resulting in an "open" rate of 27.3 percent. Further, 964 students clicked on the link embedded in the phishing message, resulting in a "click" rate of 13.3 percent. Thus, over a quarter of those students who received a phishing message opened it, and nearly a half (48.8 percent) of those who opened the email went further and clicked on the link embedded in the phishing message.

5.1 Comparisons between Message Conditions

5.1.1 Manipulation Checks

We could not test the effectiveness of our manipulation in the study sample because we only had access to participants who we deceived and who volunteered to complete the survey after following the email links. Thus, we conducted a post-hoc manipulation check study using a separate sample of students from the same university. We gave 238 students one of the eight email scenarios and asked them to rate the outcome described in the scenario on the extent to which it described an outcome that was positive or negative as they assessed it and whether it presented the opportunity to gain or lose something. Participants responded on nine-point semantic differential scales, with the poles of the scales anchored at negative (1) vs. positive (9) outcome and opportunity to lose (1) vs. opportunity to gain (9) something. Table 3 presents the results. Overall, the participants rated the gain conditions as more positive (*M*s = 6.06 vs. 4.64), *t*(236) = 4.39, *p* < .01) and as having a greater opportunity for gain (*M*s = 6.13 vs. 4.8), *t*(236) = 3.82, *p* < .01) than the loss conditions. However, we did not successfully manipulate all of the specific loss conditions. The participants clearly saw the bank card and course registrations as losses and negatively framed, but they did not see the tuition and alumni network conditions as losses and negatively framed. We negatively framed the latter two conditions as presenting the loss of an opportunity, but students did not interpret this frame as a loss. Rather, students interpreted the tuition assistance condition and alumni network conditions as more of a gain than loss opportunity. We also asked participants how motivated they would be to receive the outcome depicted in the email and how much they valued the outcome. A one-way analysis of variance (ANOVA) revealed no significant difference in motivation between the email conditions (*F*(7,230) = 2.0, *p* > .05). This finding suggests that any differences in susceptibility were not due to differences in motivation to pursue the outcome. The results of our manipulation checks suggest that the most appropriate statistical design was to compare the eight email conditions in a single-factor design.

Table 3. Results of Post-hoc Manipulation Checks

Condition	Positive (9) vs. negative (1) outcome	Gain (9) vs. loss (1)	Motivational value
Gift card	7.28	7.41	4.47
iPad Mini	6.37	6.20	3.87
Virus & firewall software	5.18	5.11	3.79
Volunteer	5.24	5.62	3.59
Course registration	2.64	2.82	4.67
Bank card	3.89	4.07	4.44
Tuition assistance	6.47	6.25	4.14
Alumni social network	5.77	6.23	3.84

5.1.2 Test of Hypotheses

Analyses examined differences in recipients' responses to the phishing messages. Table 4 presents the frequency with which recipients opened the different emails and clicked on the link embedded in the phishing messages. We found vast differences between message conditions for both open and click rates. The percent of recipients opening the email message ranged from a low of 1.9 percent for the bank card fraud email to a high of 54.4 percent for the course registration message. A chi-square test revealed significant differences between the eight email conditions ($\chi^2(8) = 617.0$, *p* < .001). Post-hoc comparisons revealed the following pattern for frequency of opening the email: course registration message > tuition assistance and free gift card > free iPad and free computer fire wall > volunteer opportunity > alumni network and bank card fraud (all *p*s < .05). The finding that over half of recipients (54 percent) opened the course registration message supports Hypothesis 1, which suggests that highly contextualized emails capture recipients' attention. In fact, the two messages that produced the highest number of email openings related to salient concerns for most students: keeping course registrations open and tuition assistance. We also contextualized the firewall, alumni network, and bank card conditions in that they were ostensibly sent from university officials and related to student concerns. These messages, however, did not lead to high open rates. Course registrations and tuition are likely to be more salient and important to college students and, hence, more likely to draw their attention. The high open rate for the course registration condition is also consistent with Hypothesis 2 (loss frames result in higher susceptibility than gain frames), but the open rate in the bank card condition, the only other loss condition identified by the manipulation check analysis, was very low. Overall, the average open rate in loss frames did not differ from that in gain frames.

Consistent with Hypothesis 3, messages that related to protecting assets (registrations and computer) or acquiring valued things or resources (iPad, gift card, and money for tuition) were likely to induce recipients to open the email messages. Messages related to social motives (volunteering and networking) were less effective. For the most part, recipients ignored the bank card protection message because, perhaps, they were familiar with similar messages and recognized them as fraudulent.

Table 4. Frequency of Opening Email and Clicking on Link by Message Condition

	Gift card	Tuition assist.	iPad	Registration	Firewall	Bank card	Volunteer	Social network
N	907	907	905	904	902	902	899	899
# open	345_d	357_d	291_c	492_e	269_c	17_a	185_b	19_a
% open	38%	39%	32.1%	54.4%	29.8%	1.9%	20.6%	2.1%
# click	194_b	187_b	178_b	338_c	40_a	3_a	20_a	4_a
% click	21.4%	20.6%	19.7%	37.3%	4.4%	< 1%	2.2%	< 1%

Note: Means with different subscripts in rows are significantly different ($p < .05$).

Results for the frequency with which recipients clicked on the embedded link in the email messages mirrored the results for opening the email. The chi-square analysis revealed significant differences between the eight conditions ($\chi^2(5) = 560.8$, $p < .001$), with the highest click rate (37.3 percent) found for the course registration message, and the lowest rate (< 1 percent) found for the bank card and social network messages. Post hoc comparisons found that the course registration message produced higher click rates than the iPad, gift card, and tuition assistance messages, which did not differ from each other but produced significantly more clicks than did the other four conditions (*p*s < .01).

5.2 Individual Differences: Gender and Major

Additional analyses examined open and click rates by major and gender across the eight message conditions. We found a main effect for gender: collapsing across all eight message conditions, females were more likely to open the email message than males; 29.9 percent of females (n = 1,051) opened their message compared to 24.4 percent of males ((n = 924), $\chi^2(1) = 22.95$, $p < .01$). However, the difference in click rates between males and females was not statistically significant ($p < .05$), with 14.1 percent of females (n = 495) clicking on the link versus 12.6 percent of males ((n = 469), $\chi^2(1) = 3.36$, $p = .067$). We conducted post hoc analyses to examine gender differences in open rates in each message condition. Using a Bonferonni adjusted p-value of .006 (for eight post-hoc tests), we found significant gender differences in open rates for the gift card and course registration conditions. As Table 5 shows, women were significantly more likely than men to open the gift card (44 percent vs. 32 percent; $\chi^2(1) = 13.5$, $p < .01$) and course registration (60 percent vs. 49 percent; $\chi^2(1) = 11.6$, $p < .01$) emails. Gender differences in the other conditions were not significant. Thus, the effect of gender on open rates was restricted to the iPad and course registration conditions.

Table 5. Open Rates by Message Condition and Participant Gender

	Gift card	Tuition assist.	iPad	Registration	Firewall	Bank card	Volunteer	Social network
Female	44.1%	41.7%	33.4%	60.2%	32.6%	1.8%	23.3%	1.8%
Male	32.3%	37.1%	31.2%	48.9%	27.2%	1.9%	18.0%	2.4%

Chi square tests also revealed a significant main effect of academic major on the frequency of opening the email ($\chi^2(3) = 12.40$, $p < .01$). Table 6 presents the frequency of openings and link clicks by student major, collapsed across all message conditions. Post-hoc comparisons revealed that business and social science majors were more likely to open the email than humanities majors. No other comparisons were statistically significant ($p < .05$). Analyses revealed no significant differences between majors in terms of click rate ($\chi^2(3) = 5.42$, $p =.14$).

Table 6. Frequency of Opening Email and Clicking on Link by Major, Collapsed Across Message Conditions

	Social science	Business	Humanities	STEM
# open	931	274	269	501
% open	27.8%	30.6%	23.8%	27.0%
# click	466	112	130	256
% click	13.9%	12.5%	11.5%	13.8%

We conducted log-linear analyses to test for higher-order interactions between condition, gender, major, and click and open rates. Results showed no significant gender *x* condition, major *x* condition, or gender *x* major *x* condition interaction terms for either click or open rates.

5.3 Survey Responses

Of the 964 students who clicked on the link in the email, 206 (21.4 percent) completed the survey on the landing webpage. There were not enough responses in each experimental condition to conduct comprehensive analyses, but we present the following results for informational purposes. Respondents reported being moderately suspicious of the email that they received (mean rating = 2.4 on a 1-4 scale) and being moderately careful in reading the email (mean rating = 2.6 on a 1-4 scale). There were no gender differences in reported suspicion or care, and having a firewall or virus protection did not affect suspicion or carefulness. A majority (59.2 percent) of respondents reported scrolling over the link before clicking on it, and 22.4 percent reported that they searched for information on sender before clicking.

We analyzed suspicion ratings for experimental conditions with more than 10 respondents. ANOVA revealed main effects of condition for suspicion and carefulness in reading email (*F*s (3,187) = 8.02 and 5.77, respectively, *p*s < .01). Post-hoc tests revealed that respondents in the gift card and tuition assistance conditions were less suspicious and read the email less carefully than those in the free iPad condition (*p*s < .05), while those in the course registration condition fell between these two groups. The only other significant effect was a main effect of condition on conscientiousness (*F*(3, 133) = 2.68, *p* = .05). Respondents in the registration and tuition assistance conditions were higher in conscientiousness than respondents in the iPad and gift card conditions, but post-hoc tests between conditions failed to reach statistical significance (*p* < .05) when we used the Tukey correction for the number of post-hoc comparisons.

The trait of conscientiousness was positively correlated with being suspicious (*r* = .25) and carefully reading the message (*r* = .21, *p*s <.05). These findings are consistent with the behavioral tendencies of conscientious people to pay close attention to details and to be planful, although the findings could also reflect a response bias. Finally, individuals reporting themselves to be high in ambition and achievement striving also reported being more suspicious of the emails (*r*s = .22 and .23, respectively, *p* < .05).

6 Discussion

In this study, we examine the impact of the content and framing of phishing emails on user vulnerability. Results suggest that the desire to protect things of value and the opportunity to obtain valued objects are motives that make people susceptible to phishing scams. Further, messages that targeted issues and concerns relevant to the student sample (e.g., course registration and tuition assistance) were most successful (i.e., in convincing the participants to click the link in the email).

6.1 Analysis of Hypotheses

In partial support of Hypothesis 1, student participants were more susceptible to a highly contextualized message pertaining to course registrations than to other generic messages. The threat of losing course registrations spurred over half of recipients to open a fraudulent email message, and over one-third of them to follow the link embedded in the fraudulent message. Of participants who opened the registration email, over two-thirds (68.7 percent) clicked on the phishing link. Thus, the contextualized message channeled recipients through the first two steps of the phishing process and lead them to read the email and click on the embedded link. This “channeling” of behavior is consistent with the heuristic-systematic model (Eagly & Chaiken, 1993) in that message cues (e.g., an important matter and a credible sender) can propel people to act without (or even despite) carefully deliberating on the consequences of their actions. We conducted this study after the advanced registration period for the upcoming semester had closed, a time when students are likely to be highly motivated to protect their course registrations. The saliency and importance of course registrations may have lowered the recipients’ sufficiency threshold and caused them to respond to the link quickly without carefully considering the email’s legitimacy. Additionally, the strongly contextualized message may have withstood initial scrutiny or skepticism from the individuals’ systematic processing system. The survey responses suggest that this may have been the case because respondents receiving the course registration email indicated they were moderately suspicious of the email but still clicked on the link. Luo et al. (2013) suggest that the most effective phishing messages would be those that can operate on both the heuristic and systematic processing systems. The threat of losing course registrations may have lowered the sufficiency threshold in students and pushed them toward quick action, while the rich context cues may have convinced those scrutinizing the message that it was authentic. The second most clicked link (tuition assistance) was also high in contextualization, which further suggests that a personalized context increases susceptibility to phishing. The extreme version of contextualization is a spear-phishing attack that appears to come from someone known to the victim and that addresses the victim by name. The results of spear-phishing studies are similar to ours. Halevi et al. (2015) found that 25 of 40 employees (62.5%) clicked on a link embedded in a fraudulent email purportedly from the company's IT manager and addressed to them individually. Our results suggest that phishing messages need not be personalized to that extent in order to be effective.

Hypothesis 2 states that loss frames increase susceptibility compared to gain frames. The results suggest that this effect may only be true for highly contextualized messages, such as the course registration email. The manipulation check analysis indicated that the only other condition that the participants interpreted as a loss frame was the bank card condition, which resulted in low open and click rates. Although the second most successful message threatened students with the loss of an opportunity for tuition assistance, the manipulation check analyses indicated that students were more likely to adopt a gain frame than a loss frame for this message.

The results also showed that the chance to acquire free goods (an iPad or gift card) increased vulnerability to phishing attacks. One in five students who received a message promising a gift card or an iPad visited the phishing website and, thus, put themselves at risk for being scammed or having the security of their computer and data compromised. This finding is consistent with the drive to acquire that Lawrence and Nohria (2002) identify as a universal emotional need in humans. The lure of "free" goods may lower the sufficiency threshold in recipients and cause them to respond in heuristic processing mode and overlook the risks associated with phishing emails. Some evidence from the post-study survey supports this explanation; respondents reported being least careful when reading the gift card message.

Participants were less susceptible to the phishing messages geared toward social outcomes (altruism and social networks) than for material outcomes. Perhaps these messages were not as believable, or participants were not highly motivated to pursue the social outcomes offered by the phishing message. University students have numerous opportunities to assist others and participate in social activities and networks, which may have reduced the attractiveness of this opportunity.

6.2 Individual Differences

We also examined how vulnerabilities change across different student populations based on academic major and gender. Previous research suggests that women are more susceptible to phishing than men (e.g., Halevi et al., 2013; 2015; Jagatic et al., 2007). We found that women were more likely than men to open phishing messages but not necessarily more likely to click on the embedded links. Perhaps women are more easily enticed to look at phishing emails (step 1 of the phishing process) but are as adept as men at detecting deceptive messaging (step 2). Likewise, business majors were more likely than humanities majors to open emails, although we found no differences in click rates by type of major. A possible explanation for this finding is that the business major at the university is very competitive and attracts highly motivated and engaged students, who may also be more diligent in monitoring and responding to emails linked to the university.

6.3 New Contributions

This study provides several important contributions to information security research. It clearly demonstrates that situational or contextual factors alter the effectiveness of phishing attempts. Users' or recipients' responses are rooted in their perceptions of risk and reward when confronted with a decision choice. Cognitive biases and heuristics, however, may reduce rational logic and increase vulnerability to fraudulent messages. Contextualized social engineering attacks, such as emails to students that threaten the loss of academic registrations, may cause them to overlook cues of deception that they might normally catch. The findings also lend support to the heuristic-systematic processing model (HSM). A contextualized message that threatens the loss of something valuable may be especially likely to prompt people to act quickly without carefully considering the potential consequences of the action. The fear associated with the anticipated loss of something valuable may increase reliance on heuristics and automatic responses (Damasio, 1984; LeDoux, 2003). However, should initial suspicion cause recipients to more systematically process a message, the rich context of the message may convince them that the message is legitimate. The survey results support this assertion by showing that respondents who clicked on the embedded link were moderately suspicious of the email but clicked on the link nonetheless. Perhaps the emotion elicited by the message—the anticipation of gaining or losing something valuable—lowered the user's sufficiency threshold for responding or influenced their appraisal of the legitimacy of the message.

The survey results also suggest that students may be aware of common phishing detection methods. Nearly 60 percent of those who completed the survey reported that they scrolled over the link in the email, and 22 percent reported that they searched for information on the Internet before clicking the link. It is difficult to draw firm conclusions from these findings because of the low response rate and because we cannot determine the veracity of responses, but the findings may indicate that young adults are aware of techniques to detect and protect against phishing. However, the study also shows that contextualized messages that mask URLs and other cues can still channel users toward fraudulent websites.

The vast difference we found in open and click rates is also noteworthy. Although the most influential email threatened the loss of something (course registration), so too did the least influential message (bank card fraud). Perhaps the latter email was less believable to students because it resembled common or known phishing attempts. The university's website, for example, presents an example of a phishing email that asks for bank information. Thus, the bank card message was similar to common phishing attempts; students may have rejected it as a common scam.

6.4 Training Implications

As the literature illustrates, past training has not been very effective, which we posit may be due to the vast array of techniques of deception (in phishing) and human cognitive limitation to process and absorb them. Creating highly focused and contextualized awareness campaigns targeted to different audiences based on their cognitive biases may improve the impact of the training provided. Given that students take emails from university administration (e.g., accounts, scholarships, etc.) and instructors (e.g., grades, assignments, and plagiarism etc.) seriously, such interventions would help provide students with ways to distinguish legitimate from illegitimate emails. Many methods exist to do so, such as: 1) ensuring that all emails come from university email addresses and that all of the links in the email start with the university domain, 2) providing a procedure for students to verify the authenticity of the email either by phone or the Web, and 3) educating students on the importance of verifying emails, especially those that request sensitive information. Additionally, given that financial incentives, even if relatively small (e.g., gift card), strongly motivate students to respond, we could educate students on ways to determine the legitimacy of offers. To create contextualized strategies, we need to understand the psychological traits of specific demographics and create appropriate messages to neutralize individual vulnerabilities.

Phishing is fundamentally a human problem, and education is a critical tool to reduce susceptibility (Jagatic et al., 2007). Anti-phishing training has been ineffective, and poor training results have led some researchers to go so far as to claim that users cannot be trusted to make rational security decisions and that those decisions should be taken out of their hands and made automatically for effective security (Görling, 2006). The conjecture that we draw from our research is that targeted training based on specific biases that increase phishing susceptibility would be effective. For example, to guard against biases that stem from heuristic processing, training might seek ways to raise the sufficiency threshold in recipients and, thereby, increase the chances that users will systematically process messages. Training also needs to counter the effects of pretexting and contextualization. It may be difficult to prevent pretexting, but users can be provided with techniques for verifying authenticity of internal communications, and organizations should develop clear policies about the types of information that might be requested of its members (e.g., "We will never ask for your password, ever"). Our future research will entail incorporating good practices based on learning science principles that are contextualized according to user motivation and psychological biases.

6.5 Limitations and Future Research

This study has several limitations. We did not ask students for personal information or data and, thus, do not know if students would have been deceived into divulging sensitive or confidential information. This is the critical third step of the phishing sequence, where users provide personal information after opening and reading the email and clicking on an embedded link. We need more research to examine vulnerability at this third stage. Nonetheless, clicking on links in emails (step 2) increases vulnerability because doing so may automatically download and install malware on the user's computer. Links can be associated with downloads of executable files that can install trojans on the user's computer without their knowledge. The participants in this study were students enrolled in a U.S. university, and users in different countries and from different cultures may behave differently in regards to phishing (Flores et al., 2015; Tembe, et al., 2014). The study focuses on general phishing attacks via emails and does not address spear phishing or phishing through different channels such as online social media platforms. Further research should investigate whether the effects of contextualized messages generalize to these other forms of phishing.

Finally, we did not have a fully balanced experimental design and our manipulation of gain/loss frame was only partly successful. However, comparisons between the eight scenarios provide insights into the effects of contextualization and framing. Future research should expand on our findings and test the effects of different scenarios in experimental settings.

7 Conclusions

We tested the premise that successful phishing attacks take advantage of the human tendency to make quick intuitive judgments based on initial impressions of the immediate context. We tested the assertion that susceptibility to phishing is strongly associated with the contextual setting of a phishing email via an experiment with emails framed based on our hypotheses to elicit user reaction. We found that the context of the email was strongly related to susceptibility to phishing and that different demographics were associated with susceptibility. The research implies the need for developing context-based education to help users detect phishing emails as an effective counter to the increasing design sophistication of phishing attacks. It also illustrates, based on rate of email opening, differences in susceptibility of different users for specific demographics features (e.g., major and gender). This finding suggests the need to identify the precise vulnerabilities based on demographic groups and provide targeted education designed for each group. In the future, we would like to examine the impact of such targeted education on reducing users' susceptibility to phishing.

References

Aaron G., & Rasmussen, R. (2015). Global phishing survey: Trends and domain name use in 2H2014. *Anti-phishing Working Group.* Retrieved February 22, 2016, from http://www.antiphishing.org/download/document/245/APWG_Global_Phishing_Report_2H_2014.pdf

Anandpara, V., Dingman, A., Jakobsson, M., Liu, D., & Roinestad, H. (2007). Phishing IQ tests measure fear, not ability. In S. Dietrich & R. Dhamija (Eds.), *Financial cryptography and data security* (pp. 362-366). Berlin: Springer.

Anderson, R., & Moore, T. (2009). Information security: Where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society A*, *367*(1898), 2717-2727.

Anderson, T. (2010). Pretexting: What you need to know. *Security Management*, *54*(6), 64-70.

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, *29*(3), 706-714.

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2015). *Breaching the human firewall: Social engineering in phishing and spear-phishing emails.* Paper presented at the 26th Australasian Conference on Information Systems, Adelaide, Australia.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *Security & Privacy*, *12*(1), 28-38.

Chaiken, S. (1987). The heuristic model of persuasion. In M. P. Zanna, J. M. Olson, & C. P. Herman (Eds.), *Social influence: The Ontario symposium* (vol. 5, pp. 3-39). Hillsdale, NJ: Lawrance Erlbaum Associates.

Chen, S., & Chaiken, S. (1999). The heuristic-systematic model in its broader context. In S. Chaiken & Y. Trope (Eds.), *Dual-process theories in social and cognitive psychology* (pp. 73-96). New York: Guilford.

Cialdini, R. B. (1993) *Influence: Science and practice*. New York: Harper Collins.

Damasio, A. (1994). *Descartes' error: Emotion, reason, and the human brain*. New York: Penguin Books.

Dhamija, R., & Tygar, J. D. (2005). The battle against phishing: Dynamic security skins. In *Proceedings of the First Symposium on Usable Privacy and Security* (pp. 77-88).

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 581-590).

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In *Proceedings of the Second Symposium on Usable Privacy and* Security (pp. 79-90).

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*. Fort Worth, TX: Harcourt.

Egelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1065-1074).

Emigh, A. (2005). *Online identity theft: Phishing technology, chokepoints and countermeasures*. Retrieved from http://www.passfaces.com/published/Phishing-dhs-report.pdf

Ferguson, A. J. (2005). Fostering e-mail security awareness: The West Point carronade. *EDUCAUSE Quarterly, 28*(1), 54-57.

Finn, P., & Jakobsson, M. (2007). Designing ethical phishing experiments. *IEEE Technology and Society Magazine*, *26*(1), 46-58.

Flores, W. R., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information & Computer Security*, *23*(2), 178-199.

Gordon, M. E., Slade, L. A., & Schmitt, N. (1986). The "science of the sophomore" revisited: From conjecture to empiricism. *The Academy of Management Review*, *11*(1), 191-207.

Görling, S. (2006). The myth of user education. In *Proceedings of the 16th Virus Bulletin International Conference*.

Halevi, T., Lewis, J., & Memon, N. (2013). *Phishing, personality traits and Facebook.* arXiv preprint arXiv:1301.7643v2.

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.*

Harrison, B., Vishwanath, A., Ng, Y. J., & Rao, R. (2015). Examining the impact of presence on individual phishing victimization. In *Proceedings of the 48th Hawaii International Conference on System Sciences* (pp. 3483-3489).

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81.

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

Jakobsson, M., & Ratkiewicz, J. (2006). Designing ethical phishing experiments: A study of (ROT13) rOnl query features. In *Proceedings of the 15th International Conference on World Wide Web* (pp. 513-522).

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y.-K. (2007). What instills trust? A qualitative study of phishing. In *Proceedings of the 11th International Conference on Financial Cryptography* (pp. 356-361).

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An emprical study. *MIS Quarterly*, *34*(3), 549-566.

Jones, N. (2015). A perfect match: Uniting mobile security with your employees' use of online dating apps. *SecurityIntelligence.* Retrieved from https://securityintelligence.com/datingapps

Kahneman, D. (2011). *Thinking, fast and slow*. New York: Farrar, Straus and Giroux.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, *47*(2), 263-291.

Kim, D., & Kim, J. H. (2013). Understanding persuasive elements in phishing e-mails: A categorical content and semantic network analysis. *Online Information Review*, *37*(6), 835-850.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. In *Proceedings of the Anti-phishing Working Groups 2nd Annual eCrime Researchers Summit* (pp. 70-81).

Kumaraguru, P., Cranor, L. F., & Mather, L. (2009a). *Anti-phishing landing page: Turning a 404 into a teachable moment for end users*. Paper presented at the 6th Conference on Email and Anti-Spam. Mountain View, CA, USA.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009b). School of phish: A real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*.

Lawrence, P. R., & Nohria, N. (2002). *Driven: How human nature shapes our choices*. San Francisco: Joseey-Bass.

LeDoux, J. (2003). The emotional brain, fear, and the amygdala. *Cellular and Molecular Neurobiology*, *23*(4-5), 727-738.

Leventhal, H. (1970). Findings and theory in the study of fear communications. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (vol. 5, pp. 119-187). New York: Academic Press.

Luo, X., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the heuristic-systematic model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28-38.

Mayhorn, C. B., & Nyeste, P. G. (2012). Training users to counteract phishing. *Work, 41*(1), 3549-3552.

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. New York: John Wiley & Sons.

Moody, G., Galletta, D. F., Walker, J., & Dunn, B. K. (2011). Which phish get caught? An exploratory study of individual susceptibility to phishing. In *Proceedings of the International Conference on Information Systems*.

Petty, R. E., & Cacioppo, J. T., (1986). The elaboration likelihood model of persuasion. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (vol. 19, pp. 123-205). San Diego: Academic Press.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (pp. 88-99).

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of Interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373-382).

Vishwanath, A. (2015). Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. *Journal of Computer-Mediated Communication*, *20*(5), 570-584.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, *55*(4), 345-362.

Watters, P. A. (2009). Why do users trust the wrong messages? A behavioural model of phishing. In *Proceedings of the eCrime Researchers Summit* (pp. 1-7).

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, *16*(6), 315-331.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662-674.

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 601-610).

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research*, *25*(2), 385-400.

Tembe, R., Zielinska, O., Liu, Y., Hong, K. W., Murphy-Hill, E., Mayhorn, C., & Ge, X. (2014). Phishing in international waters: Exploring cross-national differences in phishing conceptualizations between Chinese, Indian and American samples. In *Proceedings of the 2014 Symposium and Bootcamp on the Science of Security*.

Appendix A. Email Messages Used in the Experiment

Table A1. Financial Acquisition

Gain	Loss
From: Student Research **Subject:** $50 gift card to fill survey Dear Student: Receive $50 for completing a short survey! Ludlow Corporation has been measuring consumers' attitudes for three decades, and companies rely on our results to develop and market their products. If you complete our new survey by MIDNIGHT TONIGHT, you will receive your choice of a $50 gift card to Amazon.com or Barnesandnoble.com. Just click on the link below to complete the survey and tell us which gift you want and where to send it. http://ualbany.9nl.com/giftcardsurvey/ Best Regards,Kevin Peterson Ludlow Corporation	**From:** Financial Management **Subject:** RIAA Tuition Assistance Dear Student: Recording Association of America has provided 2000 tuition relief vouchers of $300 for students who sign a pledge to not download music illegally from the Internet. This has been provided since your University was able to successfully implement a program to curb illegal download of music from the web. The vouchers are first come first serve until they last. You must act quickly before they run out. Please click on the link below and provide your personal information. http://ualbany.9nl.com/tuitionrelief/ Best Regards, Kevin Peterson Asst VP, Financial Management

Table A2. Non-financial Acquisition / Goods

Gain	Loss
From: Apple Research Team **Subject:** Get a free iPad mini for giving it a test drive Dear Student: You've won an iPad mini! Apple is distributing its new mini tablet to select university students who are willing to help evaluate it. The tablet has the same capabilities as an iPad with a smaller screen. In return for the free tablet all we will request is for you to provide us feedback on the product every two weeks. You will be provided a template to fill out your experiences with the tablet. Apple is an equal opportunity company and you were randomly selected without any cultural or racial bias. Please register at the following link and make sure that you accept the terms and conditions at the end of the form. http://ualbany.9nl.com/ipadmini/ Best Wishes, Apple Research Team	**From:** Legal Affairs **Subject:** Action Needed to Keep your Registration Open Dear student: The University takes its legal responsibility seriously and is very concerned about illegal download of music on campus. We have been singled out by RIAA as one of the most prolific abusers of illegal music downloads. You have yet to complete the illegal downloading pledge, which the University requires. If you do not complete the form, you will have a block on your registration and will not be able to sign up for courses during the pre-registration period. Please click on the link below to complete the form. http://ualbany.9nl.com/registration/ Sincerely, Kevin Peterson Legal Affairs

Table A3. Security

Gain	Loss
From: Admin **Subject:** Students - protect your computer with a free firewall Dear Student: The University takes its information security very seriously and is concerned about the recent spate of cyber attacks on computers within the University. We would like to ensure that all student computers are secure. Any virus infection on your computer can get transmitted to the University network. We have decided to provide students with a firewall program to install on your computers. Please download the firewall on your computer. It is a simple one step process that will add to your security as well as that of the University. Please download the firewall software as soon as you can. This service will not cost you anything. http://ualbany.9nl.com/studentsoftware/ Best regards, The Information Security Office	**From:** Student Accounts **Subject:** Student Bank Card Fraud Prevention Dear Student: There have been cyber attacks at several banks that manage visa, master and debit card transactions for online purchases. The attacks have been going on since March of this year but were discovered earlier this month. We suspect that several million bank or credit card numbers have been compromised. If you have used your card for online purchases in the U.S. this year your account may have been compromised. The easiest way to see if your account has been compromised is to click the following link. If your card has been compromised you should call your bank and request a new one immediately. http://ualbany.9nl.com/FraudPrevention/ Sincerely, The Student Support Office

Table A4. Social

Gain (rewards of altruism)	Loss (potential networks)
From: USA Aid Rescue Organization **Subject:** Volunteers needed! Hi! Hurricanes Isaac and Sandy have caused significant devastation in the Gulf Coast and Atlantic Coast regions. Thousands of people have lost everything and have become homeless. The initial response by Americans was outstanding, but these people still need help. Efforts by Red Cross are limited to emergency help. Please make a donation of time or money at the following link. People need our help! http://ualbany.9nl.com/volunteer/ Kindly, USA Aid Rescue Organization	**From:** Name: Alumni Network **Subject:** UAlbany Friends Network Dear User: Don’t be left friend-less – act now to maintain membership in alumni networks. Your alumni network has established an account for you in their rapidly growing social connections with influential alumni. This network will provide access to internships in all fields of study, as well as to high paying jobs. You must confirm your account or it will be deleted. Click the following link to confirm your personal information and to retain your membership account. http://ualbany.9nl.com/UaNetwork/ Sincerely, Kevin Peterson Alumni Network Coordinator

Appendix B. Informational Message

You've Been Phished!

Dear Student:

This was an email to test whether or not you would click on a Phishing link. Fortunately, this is only a test and no harm was done to your computer or you. If this had been a real email, you could have become a victim of Phishing. Our goal is to educate students on the dangers of Phishing such that do not become victims of identity theft.

This study is completely anonymous and we do not know who you are. Even some of the most technologically savvy people become victims of such phishing attacks. We will invite you to participate in a short survey study that asks your perceptions of phishing messages. But first, we want to give you some tips to avoid getting phished. Even if you decide not to take our survey, please pay attention to these tips:

1. No legitimate firm is going to ask you for account information, passwords, verification of security questions or other sensitive information.
2. Even if the email address seems to be from a legitimate company you conduct business with it could still be a phishing email with the real address camouflaged. If the email seems suspicious, instead of replying to the email, call the customer service
3. Be especially wary of emails warning you about security breaches and account compromises asking you to provide detailed account information – these are phishing scams
4. Be extra careful of misspelled names e.g., allbany.edu instead of albany.edu or R0gers.com instead of Rogers.com. Check for the name of the company on the Internet.

If you do get phished the hacker may attempt to commit credit card fraud, bank fraud or identity theft. For such scenarios you need to take the following steps:

I. CREDIT/ATM CARD FRAUD

a) Report the theft of information to the credit card company and cancel your current card
b) Check your credit card statement to see if there are transactions you do not recognize
c) Report any unauthorized transactions to the credit card company (your liability is limited to $50)
d) Report any unauthorized transactions on your debit/ATM card within 60 days of receiving the statement (if you report within 60 days your liability is zero else it is unlimited)

II. BANK ACCOUNT THEFT

a) Call your affected financial institution to report the loss right away.
b) Cancel your account and open a new one.

III. IDENTITY THEFT

a) Request credit reports from the three agencies to see if any fake accounts have been opened on your behalf. If true request the malicious activity be removed from your records and a victim’s statement be placed on record
b) File criminal report with your local police
c) Report theft to the Social Security Administration's Fraud Hotline
d) Alert passport office to ensure that a passport is not ordered in your name
e) File a complaint to the Internet Fraud Office

To help us improve the security at the University we will appreciate if you could take a short anonymous survey that pertains to your perceptions about risk.

About the Authors

Sanjay Goel is a Professor and Chair of the Information Security and Digital Forensics Department in the School of Business, Director of Forensics Analytics Complexity Energy Transportation and Security Center, and Director of Research at NYS Center for Information Forensics and Assurance at the University at Albany, SUNY (UAlbany). Dr. Goel received his PhD from Rensselaer Polytechnic Institute and has worked at General Electric Global Research prior to starting at UAlbany. His research interests include information security, cyber warfare, complex systems, security behavior and cyber physical systems He won the promising Inventor's Award in 2005 from the SUNY Research Foundation. He has received, the SUNY Chancellor's Award and UAlbany president's award for Excellence in Teaching, UAlbany Excellence in Research Award, SUNY Chancellor's Award and UAlbany president's award for Excellence in Service, the Graduate Student Organization Award for Faculty Mentoring, and was named an AT&T Industrial Ecology Faculty Fellow He has received over 8 million dollars in research funding from: NIJ, U.S. DOE, NSF, UTRC, NYSERDA, AT&T, U.S. Department of Commerce, IARPA, AT&T Foundation, James S. McDonnell Foundation, and Blackstone Foundation.

Kevin Williams is the Vice Provost and Dean for Graduate Studies at the University at Albany, State University of New York. Prior to his current role, he served as director of undergraduate advising in Psychology from 1994-2005, graduate director from 2005-2007, and department chair from 2007-2010. He has also been area head for the industrial-organizational psychology and the social-personality graduate doctoral programs. Williams received his PhD in psychology from the University of South Carolina. His research and teaching interests focus on the application of psychology to organizational settings. He received the President's and Chancellor's Excellence Awards in Teaching and an excellence in undergraduate advising in the psychology department. His major areas of research are (1) human motivation and performance, where he studies the self- regulatory processes that guide goal strivings and goal revision over time; (2) the psychology of blame, where his work explores the social-cognitive processes that underlie the allocation of blame for accidents; and (3) employee assessment and appraisal, where his work seeks to identify best practices for assessing and evaluating employee aptitude and performance.

Ersin Dincelli is a doctoral candidate in the Department of Informatics and an adjunct professor in the Department of Information Technology Management at the University at Albany, State University of New York. He works as a senior research analyst at the New York State Center for Information Forensics and Assurance (CIFA) focusing on multiple research projects including investigating cultural and socio-psychological impacts on information security and privacy behavior, behavioral differences on online social networks, cybersecurity education, and complex systems. He received his MBA with a specialization in Information Technology Management from the University at Albany, and his BA in Economics from Uludag University in Turkey. His primary research interests include individual behavior in the context of information security and privacy, cybersecurity, cross-cultural issues in information systems, and social media data analytics.