ABSTRACT

Title of Document:	AN EMPIRICAL ASSESSMENT OF USER ONLINE SECURITY BEHAVIOR: EVIDENCE FROM A UNIVERSITY
	Sruthi Bandi, Master of Information Management, 2016
Directed By:	Dr. Michel Cukier, A. James Clark School of Engineering Dr. Susan Winter, College of Information Studies

The ever-increasing number and severity of cybersecurity breaches makes it vital to understand the factors that make organizations vulnerable. Since humans are considered the weakest link in the cybersecurity chain of an organization, this study evaluates users' individual differences (demographic factors, risk-taking preferences, decision-making styles and personality traits) to understand online security behavior. This thesis studies four different yet tightly related online security behaviors that influence organizational cybersecurity: device securement, password generation, proactive awareness and updating. A survey (N=369) of students, faculty and staff in a large mid-Atlantic U.S. public university identifies individual characteristics that relate to online security behavior and characterizes the higher-risk individuals that pose threats to the university's cybersecurity. Based on these findings and insights from interviews with phishing victims, the study concludes with recommendations to help similat organizations increase end-user cybersecurity compliance and mitigate the risks caused by humans in the organizational cybersecurity chain.

AN EMPIRICAL ASSESSMENT OF USER ONLINE SECURITY BEHAVIOR: EVIDENCE FROM A UNIVERSITY

By

Sruthi Bandi

Thesis submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfilment
of the requirements for the degree of
Master of Information Management
2016

Advisory Committee:

Dr. Susan Winter, Co-chair

Dr. Michel Cukier, Co-chair

Dr. Brian Butler, Committee Member

Dr. Jessica Vitak, Committee Member

ACKNOWLEDGEMENTS

This thesis journey has been a challenging yet an immensely gratifying and a very rewarding learning experience. I would like to take this opportunity to thank everyone who have made this happen.

Foremost, I would like to thank my advisors, Dr. Michel Cukier and Dr. Susan Winter, who have not only served as my thesis chairs, but also guided, challenged, and encouraged me throughout the process. My advisors and other committee members, Dr. Brian Butler and Dr. Jessica Vitak have patiently assisted me and offered extremely valuable insights from varied perspectives, which has always challenged me to perform better. Thank you all for the extensive guidance.

I would like to thank my research team, Dr. Josiah Dykstra and Amy Ginther, who were instrumental in the design and execution of this study. Thank you for the persistent support and valuable feedback. I truly appreciate you both taking effort and time to read and edit the thesis drafts. A special thanks to you Amy for all the hard work on the infinite number of approvals and data requests. I couldn't have done it without you. I would also like to thank Margaret, Anmol and Fiona for the help on the writing.

I would like to ackowledge the funding from the Department of Defense for my research. I would also like to thank the members in the Division of IT for providing me with the required data and infrastructure to carry out the study.

I owe my deepest thanks to my family – the Bandi's, the Chikkam's and the Cheruvu's – for their hope in my quests and unconditional love. In particular, my pillars of strength, Amma, Nanna, Aadi and Chintu for always believing in me and standing by my side. The belief they have in me is what drives me everyday and I can never thank them enough in my life.

TABLE OF CONTENTS

List of Tables

List of Figures

1. Introduction

Cybercrime is a persistent problem, and the increase in the victimization of users in recent years is alarming (Interpol, 2015). A 2013 survey from the Pew Research Center reveals that 11% of Internet users have experienced theft of vital personal information, and 21% had an email or social networking account compromised (Rainie et al., 2013). The continual increase in the detection of information security compromise incidents emphasizes this unrelenting problem. PricewaterhouseCoopers (PWC), in its annual Global State of Information Security Survey, reports an overall 38% increase in detection of security incidents in 2015 from 2014 (PWC, 2015). The survey also noted that employees are the most-cited source of cybersecurity compromise in the organizations.

Human vulnerability is widely accepted as a significant factor in cybersecurity. Recently, a *Wall Street Journal* story asserted that humans are the weakest link in the cybersecurity chain, and that this weakest link can be turned into the strongest security asset if the right actions are taken (Anschuetz, 2015). To understand how this weakest link, the user, could be turned into a strongest asset, it is important to examine the underlying factors that influence user cybersecurity behavior.

There are broad categories of cybersecurity attacks ranging from money laundering to social engineering fraud (Interpol, 2015) that take advantage of the human vulnerabilities in cybersecurity. For example, social engineering frauds involve scams used by criminals to deceive the victims into giving out personally

identifiable information or financial information. Phishing is one of the most common kinds of cybersecurity attacks and is used as an example here (US-Cert, 2013). Phishing attacks use fake websites, emails or spam to lure and capture a person's personal information. Phishers take advantage of the Internet and its anonymity to commit a diverse range of criminal activities. The types of phishing attacks are evolving over time and the Anti-Phishing Working Group, a coalition unifying the global response to cybercrime across industries, states in their latest report that as many as 173,262 unique phishing reports have been submitted in the fourth quarter of 2015 (Anti-Phishing Working Group, 2016). These attacks are particularly sensitive to human reactions because for an attack to be successful, the human target must fall for the deception. Hence, it is very important to study and understand human behavior to reduce the damages of phishing and similar cybersecurity attacks.

Falling for cybersecurity attacks such as phishing involves a user deciding to click on a link or reply to an email; hence, understanding technology-based decision-making processes should help understand why individuals fall victim to phishing scams and similar cybersecurity attacks. Psychology researchers have studied how individual differences affect decision-making, and specifically how a particular behavior is correlated with individuals' attitudes towards risk (Appelt et al., 2011). If some individual factors are also predictive of user security behavior, then those factors can be emphasized to customize security training and to improve outcomes.

However, studying and analyzing human behavior that poses a threat to the organization's cybersecurity in real-world situations is challenging, since most organizations do not make data about their cybersecurity attacks and compromises

publicly available. This study represents a unique opportunity to conduct research into the population of a large public university in the mid-Atlantic region of the United States that has been a repeated object of phishing attacks, and understand the various factors that could impact decision-making and user security behavior.

The overarching research question that drives this study is, "What are the factors that influence users' online security behavior?" The user security behaviors related to online security such as securing devices, generating good passwords and updating them, being proactively aware of cybersecurity threats and keeping software up-to-date are examined in this thesis. Relationships between the individual differences in users (risk-taking preferences, decision-making styles, personality traits, and demographics) and these online security behaviors are explored. Users' falling for phishing is one of the top concerns for the university studied, and hence a group of identified phishing victims are studied to gain insights into the factors that may have influenced their victimization.

This study moves beyond existing literature on user online security behavior and individual differences by including personality traits and university-level demographic factors that have not been previously investigated. While we studied online security behaviors applicable to general users' online behaviors (which includes personal devices too), such behavior relates to organizational cybersecurity because of the connectivity of devices in today's world and the freedom of connecting personal devices to an organization's network. For example, practices like BYOD (Bring Your Own Device) at work enables employees to use their personal devices in the organization. With such interconnectivity of devices, users' online security

behaviors will impact organizational cybersecurity.This study, based on the findings from the relationships between individual differences and online security behaviors, and insights from interviews with identified phishing victims, makes recommendations that can be adopted in similar organizations to create better security messaging strategies to achieve higher end-user organizational cybersecurity compliance.

2. Literature Review

This section begins with explaining the online user security behaviors that are examined in this study: securing devices, generating good passwords and updating them, being proactive aware of cybersecurity threats and keeping software up-to-date. It further describes the individual differences in risk-taking preferences, decision-making styles, personality traits and demographics. Since the exploration of how these individual differences in terms of psychometrics correlate with security attitudes and behaviors has only very recently begun (Egelman et al., 2015), this thesis draws heavily on the phishing literature as it is the best developed research stream on behavioral decision-making and cybersecurity addressing the human element. Therefore, inferences are drawn from the phishing literature on the personality traits, decision-making styles, risk-taking preferences and demographics to build the research model linking individual differences to online security behaviors.

2.1. User Security Behavior

There are three broad categories of user behaviors that are related to security behavior: Risk-averse behavior, naive or accidental behavior, and risk-inclined behavior (Stanton et al., 2005). For example, leaving a computer unattended or accessing dubious websites can be categorized as naive behavior, while always logging off the computer when unattended or changing passwords regularly can be categorized as risk-averse behavior (Pattinson and Anderson, 2007). Risk-inclined or deliberate behavior would include behaviors such as hacking into other people's accounts or writing and sending malicious code (Pattinson and Anderson, 2007).

The subset of user security behaviors considered in this study – securing devices, generating good passwords and updating them, being proactive aware of cybersecurity threats and keeping software up-to-date – fall under the categories of risk-averse and naive behavior.

Vendors include features in many of their devices that allow them to be "locked" making them unusable without a PIN or password. Often these features must be enabled by the user. Enabling these features increases the users' online cybersecurity. *Device Securement* corresponds to such behaviors as locking one's computer and mobile device screens or using a PIN or password to lock one's devices (Egelman et al., 2015).

Online account vendors emphasize the importance of generating strong passwords and updating passwords regularly to ensure security of the accounts. Most vendors encourage creation of strong passwords by mandating the usage of at least one special character, or by forcing alpha-numeric usage in the passwords. *Password Generation* in this study refers to the practices of choosing strong passwords, not reusing passwords between different accounts, and changing passwords (Egelman et al., 2015).

With the exponential growth of cyber threats, creating and promoting awareness of these threats is a key agenda for organizations world-wide (PWC, 2015). For example, in phishing attacks, the victimization involves a user's decision to click on a spurious link and falling victim to the attack. *Proactive Awareness* indicates the users paying attention to contextual clues such as the URL bar or other browser

indicators in websites or email messages, exhibiting caution when submitting information to websites and being proactive in reporting security incidents (Egelman et al., 2015).

Software vendors often provide customers with security patches and updates to keep their systems from being less vulnerable to cyber attacks. In most of these updates, a user must make the decision of choosing to update when prompted. Applying these patches and updates enables higher online cybersecurity. *Updating* measures the extent to which someone consistently applies security patches or otherwise keeps their software up-to-date (Egelman et al., 2015).

Examining and understanding the factors that influence these online security behaviors of device securement, password generation, proactive awareness and updating will enable identification of organizational IT users who may be creating vulnerabilities that can be exploited. As shown in Figure 1, there are many factors that influence user security behavior. Since the aim of this thesis is to understand the end-user cybersecurity behavior and not the overall organizational security, the focus is on the users' decision-making skills and not on the other factors like policies, values and standards.

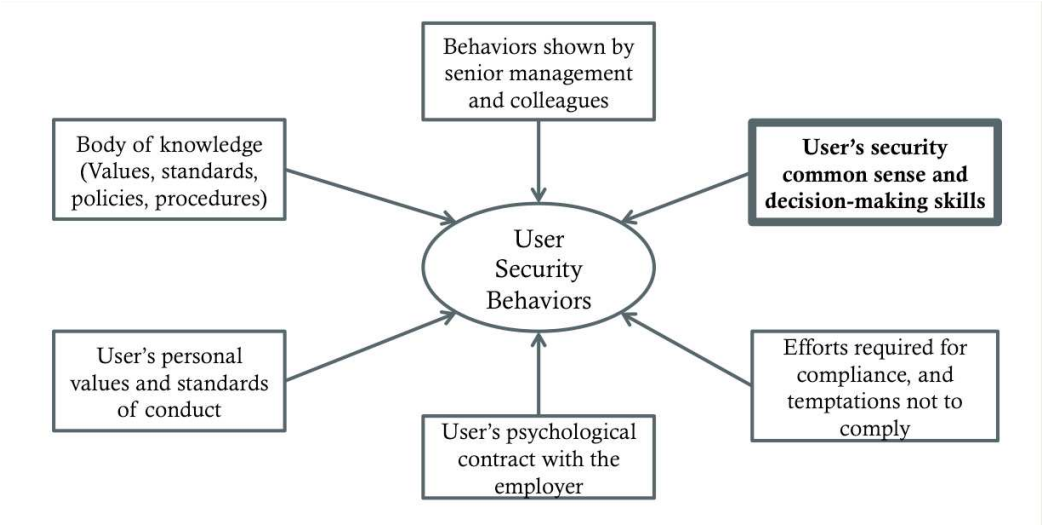

Figure 1: The factors that influence user security behavior (taken from Leach, 2003)

2.2. Decision-Making

Decision-making and user behavior that relate to general cybersecurity have been most extensively studied in connection with decision strategies and perceived/observed susceptibility to phishing (Ng et al., 2009; Leach, 2003). So we draw on this literature to guide hypothesis development. Understanding the individual differences in users that affect their decision to perform a security behavior will enable customization of security training to improve outcomes (Blythe et al., 2011). The Decision-making Individual Differences Inventory (DIDI) lists an extensive set of individual differences measures of risk attitudes and behavior, decision styles, personality traits, etc. (Appelt et al., 2011). Three sets of individual differences or psychometrics from DIDI – risk-taking preferences, decision-making styles and personality traits – are studied extensively in relation to phishing. The following sections explain these individual differences in detail and their application to online security behavior.

2.3. Risk-taking Preferences

Risk-taking is a measure of risk attitude and shapes decision-making, which is examined in the literature in relation to several forms of risky behavior (Arnett, 1996). In a study evaluating risk-taking behaviors, Charness et al., (2013) found that risk-taking attitudes correlated with self-reported risky behavior (e.g., gambling and drug use), impulsivity, and sensitivity. Sensation seeking, dangerous driving habits, and risky sexual behavior are a few of the forms of risky behavior identified in relation to risk-taking.

In relation to online security behaviors, five dimensions of risk-taking preferences have been studied: ethical, financial, health or safety, recreational, and social. A study of the associations between risk-taking attitudes and security behavior found that willingness to take health/safety risks is inversely correlated with having proactive security awareness (Egelman et al., 2015). While this study establishes a relation between health/safety risk-taking and online security, another study shows that the five dimensions of risk-taking do not significantly correlate with susceptibility to phishing (one of the most common forms of cybersecurity breaches that rely on user decision-making) (Sheng et al., 2010).

Furthermore, literature on risk awareness and phishing suggest that susceptibility to phishing is not due to lack of awareness of the phishing risks and that real-time response to phishing is hard to predict in advance by online users (Halevi et al., 2013). Downs et al. (2007) concluded that awareness of risk is not a useful strategy in identifying phishing emails; this contradicts Egelman et al.'s (2016) findings that higher proactive awareness correlates positively with correctly

identifiying a phishing website. Downs et al., (2007) also suggest that people manage risks they are most familiar with, but do not appear wary of unfamiliar risks. A two-stage experiment through a spear-phishing attack technique revealed that cyber-risk aware people surprisingly tend to fall for phishing more. Hence there is contradictory evidence in the literature that links risk-taking and awareness of risks with cybersecurity victimization.

2.4. Decision-Making Styles

Decision-making styles are the response patterns exhibited by an individual in a decision-making situation (Thunholm, 2004). Decision-making styles are generally categorized into five broad categories: rational, avoidant, dependent, intuitive, and spontaneous. The rational decision-making style can be briefly explained as using logic when making decisions. Avoidant refers to delaying decision-making. Outcome defines the style in which decisions are made by looking to others. Intuitive style includes making decisions based on instincts. Spontaneous style describes making quick decisions (John et al., 2008).

Decision-making styles appear to be an important factor in determining user online security behavior. There is little literature on the relations between decision-making style and user security behavior. One study exploring the relationship between these decision-making styles and security behaviors found that users who are less avoidant in decision-making style tend to have better security practices (Egelman et al., 2015). The study also suggests that people scoring low on dependent style scored high on awareness of security behavior. There were also significant

correlations found between rational and spontaneous decision-making styles and security behaviors (Egelman et al., 2015).

2.5. Personality Traits

Personality traits are another important factor that is extensively studied in the literature in connection with decision-making. Since, to the best of our knowledge, there are no studies that have examined relationships between personality traits and online security behaviors, we draw on the literature of personality and phishing. The following paragraphs explain the findings from the literature on relationships between personality and phishing.

The personality traits that have been studied extensively in predicting how users respond to phishing emails are: Agreeableness, Conscientiousness, Neuroticism, Openness, and Extraversion; these are generally referred to as Big Five personality factors and are widely accepted in the literature to be stable personality traits (John et al., 2008). Agreeableness is a measure of the quality of the relationships a person has with others. Conscientiousness comprises self-discipline, dutiful action, and a respect for standards and procedures. Neuroticism relates to characterisitics of anxiety, fear, anger, etc. Openness is the desire to seek out new experiences without anxiety and an appreciation of different ideas and beliefs. Extraversion is the tendency to seek out the company of others and reflects energy and positive emotions in one's personality (John et al., 2008).

Few studies have examined the relationship between personality factors and user online security behaviors that pose cyber risk to organizations, among them, there is no consensus in findings. One study found that women victims of a phishing

experiment were high on the neuroticism factor, while no significant correlation with men and neuroticism rating was found (Halevi et al., 2013). It was also found that people who score high on the openness factor tend to both post more information on Facebook as well as have more open privacy settings, which may make them more susceptible to attacks. On the contrary, another study found high openness and extraversion were related to decreased phishing susceptibility (Pattinson et al., 2012). This contradiction is puzzling, as it would seem that individuals who are generally extraverted and open to new experiences might be more likely to trust inauthentic emails.

Risk-avoidance is another personality trait in the decision-making individual differences inventory (Appelt et al., 2011). Although there are studies that looked at home computer user security awareness in avoiding phishing threats (Arachchilage et al., 2014), risk-avoidance as a personality trait is not studied in relation to other online security behaviors, but may be relevant.

From the above studies, it is evident that there is contradictory evidence, and the studies lack generalizability of factors that relate to online security behavior with risk-taking preferences, decision-making styles and personality traits. In addition, there is an essential need to leverage such knowledge at the university level and to explore demographic factors. Thus, more empirical work remains necessary in this intersection.

2.6. Demographic Factors

This section describes findings from previous research on the relationships between demographic factors and online security behavior.

Regarding password habits and management, findings from Shay et al. (2010) suggest that women are significantly more likely to reuse passwords than men. Also, individuals in the age group 18-24 are more likely to reuse passwords than individuals from any other age group with the majority of them admitting to reusing passwords across multiple sites. Further, we look at findings from the literature on relationships between demographics and phishing susceptibilities to build on the research model for studying demographics in relation to online security behaviors.

Studies on demographics and phishing susceptibility show that susceptibility to phishing attacks varies mainly with people's age and gender. A 2010 study that analyzed the demographics in relation to phishing susceptibility found that individuals in the 18-25 age group were most vulnerable to phishing attacks (Sheng et al., 2010). Parrish et al. (2009) also found that younger people, specifically college students, are more susceptible to phishing due to having lesser prior negative experience with online scams. A large-scale phishing attack study of 10,917 members of a university contradicts earlier findings of linear predictability of susceptibility with age and suggesting that the user demographics, age and gender are not conclusive alone in predicting users' susceptibility to phishing attacks (Mohebzada et al., 2012). With regards to educational background, earlier research has found liberal arts students to be more vulnerable to phishing attacks than technology and science students (Darwish et al., 2012).

In summary, the literature reviewed on risk-taking preferences suggests that health/safety risks correlated with weaker security behaviors. This thesis however looks at the remaining domains of risk-taking: ethical, financial, recreational and social to explore relationships with online security behaviors. . Avoidant and dependent decision-making styles correlated with weaker online security behaviors. In this thesis, the other three styles of decision-making, rational, intuitive and spontaneous which have not been previously studied are included because these styles have been found to impact phishing susceptibilities, and may be relevant in predicting online security behaviors. The personality traits of extraversion, conscientiousness, neuroticism, and openness are again found to be important in predicting phishing susceptibilities. Hence, in this thesis, the above traits will be examined for their relationship with online security behaviors. In addition, this study will also explore the personality traits of agreeableness and risk-avoidance.

There are a number of demographic factors associated with phishing susceptibilities and password management. Younger people have been found to be more prone to fall for phishing and are more likely to have bad password habits including password reuse. There is contradictory evidence regarding the relation of gender to security behaviors. The majority of the evidence has found that women were more likely to have weaker security behaviors. Educational background may also matter, as those in more technical tracks gain valuable experience related to online security compared with those in the arts and humanities. These findings will be extended by studying the risk-taking preferences, decision-making styles and personality traits to four security behaviors of device securement, password

generation, proactive awareness and updating. In addition, this study will include demographics of citizenship, and employment length, and test for differences between student and faculty/staff status.

3. Research Model and Hypothesis

In order to better understand the individual differences that influence users' online security behaviors, quantitative data was collected from a survey distributed to a random sample of email account holders at a large public university in the mid-Atlantic United States, and qualitative data was collected from interviews with a sample of phishing victims in the university. The primary focus of quantitative data collection was to understand the individual differences of decision-making (risk-taking preferences, decision-making styles, personality traits, demographics) and their relationship to the online security behaviors of the individual (university students, faculty, staff). The qualitative data collection was aimed at identifying strategies or changes that can be employed to achieve effective security messaging. The findings from the quantitative and qualitative data analysis are used to make recommendations for security messaging that can result in greater compliance with policies and improve overall organizational cybersecurity.

3.1. Thesis statement

Identifying individual differences in users that influence their decision-making and security behavior will enable us to propose better security messaging strategies to achieve higher organizational security.

3.2. Research Questions

Over-training those who are naturally good at maintaining online cybersecurity may cause annoyance, while under-training those who are poor at such a task can be disastrous. Understanding the factors that lead to such differences would enable

development of better awareness and training tools catering to the diverse user needs. The overarching research questions that guide this study are:

1. What individual differences in users (risk-taking preferences, decision-making styles, personality traits and demographic factors) uniquely influence their online security behavior?

2. Do users' online security behaviors vary across specific demographic factors?

3.3. Research Model

Figure 2 below depicts the research model that is tested in this thesis. Predictor variables are divided into four broad categories: Risk-Taking preferences (Ethical, Financial, Health/Safety, Recreational, Social), Decision-Making styles (Rational, Intuitive, Outcome, Avoidant, Spontaneous), Personality traits (Agreeableness, Conscientiousness, Neuroticism, Openness, Extraversion, Risk-Avoidance), and Demographic factors (Age, Gender, Role, Major, Citizenship, Employment Length).

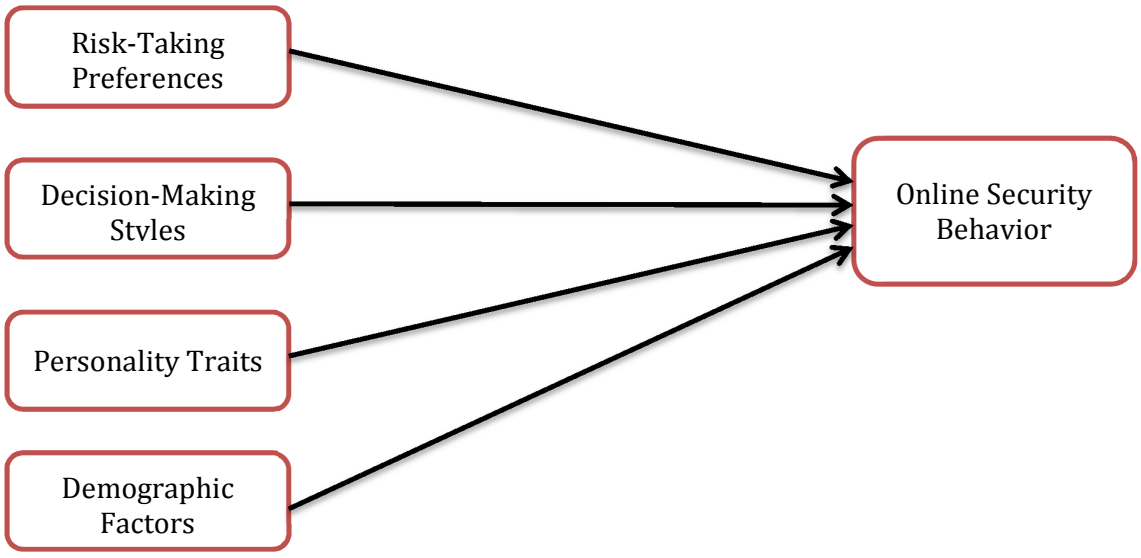

Figure 2: Research Model

3.4. Hypotheses

Drawing on the extant literature described avove, the following set of hypotheses are tested in this study.

The background research shows relations between ethical, health/safety and social risk-taking to security behaviors. In this study, financial and recreational risk-taking will also be explored for associations with users' online security behavior. In general, this study posits that people who have high risk-taking preferences in the above five domains will have weaker online security behaviors. In the following set of hypotheses, online security behaviors include device securement, password generation, proactive awareness, and updating.

H1: Users' willingness to take risks will significantly correlate with their online security behaviors.

H1a: Users who are more willing to take ethical risks will likely have weaker security behaviors than those not willing to take such risks.

H1b: Users who are more willing to take financial risks will likely have weaker security behaviors than those not willing to take such risks.

H1c: Users who are more willing to take health/safety risks will likely have weaker security behaviors than those not willing to take such risks.

H1d: Users who are more willing to take recreational risks will likely have weaker security behaviors than those not willing to take such risks.

H1e: Users who are more willing to take social risks will likely have weaker security behaviors than those not willing to take such risks.

Previous research shows relations between rational, dependent, avoidant and spontaneous decision-making styles, and online security behavior. In this study, we will also explore intuitive decision-making style for associations with users' online security behavior.

H2: Users' decision-making styles will significantly correlate with their online security behaviors.

H2a: Users who score low on rational decision-making style will more likely have weaker security behaviors than those who score high on such style.

H2b: Users who score high on intuitive decision-making style will more likely have weaker security behaviors than those who score low on such style.

H2c: Users who score high on dependent decision-making style will more likely have weaker security behaviors than those who score high on such style.

H2d: Users who score high on avoidant decision-making style will more likely have weaker security behaviors than those who score low on such style.

H2e: Users who score high on spontaneous decision-making style will more likely have weaker security behaviors than those who score low on such style.

Previous research shows relations between neuroticism, openness, extraversion and phishing susceptibility. In this study, conscientiousness, agreeableness and risk-avoidance personality traits will also be explored for associations with users' online security behaviors.

H3: Users' personality traits will significantly correlate with their online security behaviors.

H3a: Users with higher agreeableness will be less likely to have weaker security behaviors.

H3b: Users with higher conscientiousness will be less likely to have weaker security behaviors.

H3c: Users with higher neuroticism will be more likely to have weaker security behaviors.

H3d: Users with higher openness will be more likely to have weaker security behaviors.

H3e: Users with higher extraversion will be less likely to have weaker security behaviors.

H3f: Users with higher risk-avoidance will be less likely to have weaker security behaviors.

Previous research shows relations between demographic differences in age, gender and educational background, and, phishing susceptibility and security behavior. In this study, we will also explore demographic factors including role, citizenship and employment length for associations with online security behaviors.

H4: Users' demographics will significantly correlate with their online security behaviors.

H4a: Younger users will have weaker security behaviors than older users.

H4b: Female users will have weaker security behaviors than male users.

H4c: Students will have weaker security behaviors than faculty/staff.

H4d: Students pursuing rngineering and technical majors will have stronger security behaviors than those pursuing non-technical majors.

H4e: U.S. Citizens will have stronger security behaviors than non-U.S. Citizens.

H4f: User's who have been employed at the university for a longer time will have stronger security behaviors.

4. Methods

To address the research questions and inform recommendations on security messaging, the following data collection activities have been performed:

- A random sample of 4000 students, staff, and faculty were invited to take an online survey on users' risk-taking preferences, decision-making styles, personality traits and online security behaviors.
- The survey invitation was also emailed to a second sample of 304 phishing victims identified from historical data obtained through the university.
- Demographic factors of age, gender, role, major, citizenship, and employment length with the university were obtained from the campus human resources and registrar units.
- Interviews were conducted with seven victims of a prior phishing attack from the university to discuss their cybersecurity awareness and identify strategies or changes that could inform security messaging to achieve greater cybersecurity compliance.

See Appendix A for the survey instrument and Appendix B for the interview protocol.

4.1. Procedures

The following sections explain the procedures that have been utilized during the research phases of problem development and data collection.

4.1.1. Surveys

Institutional Review Board (IRB) approvals were received for the developed survey instrument. Participants were invited by email and were directed to an online survey hosted on the Qualtrics platform. They were given a consent form with details of the study explained in the standard IRB format. If they agreed to participate, they were taken to the survey, where there were a set of questions on their risk-taking preferences, decision-making styles, personality traits, demographics, and online security behaviors. The questions were not mandatory and hence the participants could skip questions that they did not want to answer. The total time taken for completion of the survey ranged from 12-20 minutes.

The survey was kept active for a three-week period with two intermediate email reminders sent. At the close of the survey, a total of 385 complete responses and 150 partially complete responses were obtained. The partial responses had very minimal information and hence were discarded from the analysis. The 385 responses from the survey were cleaned for inconsistencies and missing values, producing 369 responses that could be analyzed, consisting of 348 responses from the random sample and 21 responses from the known phishing victims sample.

4.1.2. Interviews

IRB approval was received for the developed interview protocol. A total of 185 interview invitations were sent via email from the historical data on phishing victims. The interview invitations were followed up with reminder requests to participate in the study. Seven interviews with phishing victims were conducted and audio-recorded. Interviews were conducted face-to-face and, on average, lasted about 45

minutes. The interviews included questions about each participant's recall of the incident, risk awareness, computer and Internet security practices, and insights into what could be effective cybersecurity education. The interviewers maintained observation forms to note the key points and themes from the interviews. The interviews were transcribed through a third-party service. Due to the low response rate and diversity in the participants' victimization experiences, theory building was not appropriate for this scenario. Hence, descriptive open content coding was used to identify the issues, gain insights into what could have helped the victims, and thereby propose possible solutions.

4.2. Measures

The following section discusses the measures that were used for data collection in the surveys and interviews.

4.2.1. Surveys

The measures and coding schemes of the predictor and outcomes variables in the research model are presented in the following sub-sections.

4.2.1.1. Predictor Variables

There are four sets of predictor variables: risk-taking preferences (ethical, financial, health/safety, recreational, social), decision-making styles (rational, intuitive, dependent, avoidant, spontaneous), personality traits (agreeableness, conscientiousness, neuroticism, openness, extraversion, risk-avoidance) and demographics (age, gender, role, major for students only, citizenship, employment length for staff and faculty only).

Risk-Taking preferences

The Domain-Specific Risk-Taking (DOSPERT) inventory was used to measure ethical, financial, health and safety, recreational, and social risk-taking (Appelt et al., 2011). The DOSPERT scale is a psychometric scale designed to assess risk-taking preferences through self-reporting in the above five domains. It is a 30-item assessment with 5 sub-scales for five domains using a 7- point Likert scale ranging from 'Very Unlikely' to 'Very Likely'. Each sub-scale has six individual questions and the sub-scale composite score is computed by averaging the six individual question scores. Hence, the five continuous variables were computed with scores ranging from 1 to 7.

Decision-Making styles

The General Decision Making Style (GDMS) questionnaire was used to measure rational, intuitive, dependent, avoidant and spontaneous decision-making styles (Appelt et al., 2011). GMDS is a widely used scale in the literature designed to assess how individuals approach decision situations. It is a 25-item scale with 5 sub-scales using 5- point Likert ratings from 'Strongly Disagree' to 'Strongly Agree.' Each sub-scale has five individual questions and the sub-scale composite score is computed by averaging the five individual question scores. Hence, the five continuous variables were computed with scores ranging from 1 to 5.

Personality Traits

The International Personality Item Pool **(**IPIP) has an inventory of scales that can be used to measure personality traits. The IPIP 10-item scales of neo-five domains were

used to measure agreeableness, conscientiousness, neuroticism, openness, and extraversion, and and Tellegen's multi-dimensional personality questionnaire of harm avoidance was used to measure risk-avoidance (Appelt et al., 2011). Each of the personality traits considered in our research model has positive-keyed questions and reverse-keyed questions, totaling to form a 60-item scale with 5-point ratings ranging from 'Very Inaccurate' to 'Very Accurate.'

Reverse-keyed questions were recoded by subtracting the question scores from 6 (e.g. 5 rating on a reverse-keyed question was converted to 1 rating (6 minus 5), 4 rating to a 2 rating (6 minus 4)). Averaging was used on recoded variable ratings for reverse-keyed questions and ratings for positive-keyed questions to create composite scores for each of the four outcomes. Hence, the six continuous variables were computed with scores ranging from 1 to 5.

Demographic factors

The demographics factors considered in the study include age, gender, role, major, citizenship, and employment length. The above variables were coded into simple categorical variables for ANOVA analysis, and were retained as continuous for multiple regression analysis.

Age was divided into six groups:

- Group 1: 18-25 years
- Group 2: 26-35 years
- Group 3: 36-45 years
- Group 4: 46-55 years
- Group 5: 56-65 years

- Group 6: 65+ years

Gender was retained as male and female.

Role in the university is broadly divided into two groups, students and faculty/staff.

Specific Major initially was considered as the variable, but due to too many variations and an unequal spread of responses, the responses for subgroup of students were broadly categorized into four categories of colleges/majors:

- Group 1: University students majoring in Humanities
- Group 2: University students majoring in Business
- Group 3: University students majoring in Behavioral sciences
- Group 4: University students majoring in Engineering

Citizenship is broadly categorized into two categories, 'U.S. Citizen' and 'Non-U.S. Citizen'.

Employment length was considered only for the subgroup of faculty/staff and represents the number of years since their original hire date in the university. The responses were categorized into four broad categories:

Group 1: 0-5 years

Group 2: 6-10 years

Group 3: 11-20 years

Group 4: 20+ years

4.2.1.2. Outcome Variables

There are four outcome variables in the model: device securement, password generation, proactive awareness and updating.

Online Security Behaviors

This set of variables measures online security behaviors toward securing devices, creating and reusing passwords, having proactive awareness, and keeping software up-to-date. The Security Behavior Intention Scale (SeBIS) (Egelman et al., 2015) used for measuring the users' security behavior is a 16-item scale with four subscales consisting of questions with 5-point ratings ranging from 'Never' to 'Always', to obtain self-reported data on users' online security behaviors.

SeBIS has reverse-keyed questions which were recoded by subtracting the question scores from 6 (e.g. 5 rating on a reverse-keyed question was converted to 1 rating (6 -5), 4 rating to a 2 rating (6-4)). Averaging was used on recoded variable ratings for reverse-keyed questions and ratings for positive-keyed questions to create composite scores for each of the four outcomes. Hence, the four outcomes had scores ranging from 1 to 5.

Any respondent with missing data on an outcome measure was dropped from the analysis. The SeBIS scale is a relatively new scale and hence we performed a factor analysis on the collected survey data to establish validity and reliability.

4.3. Data Analysis

A correlation analysis was performed on all the variables in the model to evaluate the data for multi-collinearity issues. For variables that appeared similar, weaker variables were dropped from the analysis. For example, the variable recreational risk-taking was highly correlated with risk-avoidance. Due to high collinearity ($r=-0.769$, $p<0.01$), recreational risk-taking was dropped from the analysis.

Factor analysis was performed on the SeBIS scale as it is a relatively new scale. Reliability testing was performed on all four of the scales that were used in the analysis. All of the scales showed moderate to excellent reliability (see section 5.1).

To answer research question 1, step-wise multiple regressions were run for each of the four outcome variables. Each step contained a group of predictor variables based on the research model (risk-taking preferences, decision-making styles, personality traits and demographics) to compute the unique variance in the outcome variables attributable to each group of predictor variables.

To answer research question 2, predictor variables from the demographic factors were tested against the four outcome variables using ANOVA along with post-hoc analysis to look for differences in outcome variables for various groups of predictor variables.

Finally, non-response analysis was performed to test for non-response bias. Response and non-response demographic samples were compared to test for statistical significance of differences in the samples.

5. Results

Below are the results based on the 369 valid responses. Findings and results from the hypothesis testing are presented in the following sections.

5.1. Factor Analysis and Reliability Testing

Principal component analysis with varimax rotation was performed on the SeBIS to verify the factor loadings onto the four sub-scales of SeBIS. Table 1 shows the factor loadings on four factors and the factor structure closely resembled that found in the original scale.

Table 1: Factor loadings for 16 items of the SeBIS scale (N = 369)

	Device Securement	**Password Generation**	**Proactive Awareness**	**Updating**
When I'm prompted for a software update, I install it right away.				0.78
I try to make sure the programs I use are up to date.				0.826
I manually lock my computer screen when I step away from it.	0.375	0.333		0.39
I set my computer screen to automatically lock if I don't use it for a prolonged period of time.	0.725			
I use a PIN or passcode to unlock my mobile phone.	0.682			
I use a password/passcode to unlock my laptop or tablet.	0.748			
If I discover a security problem, I continue what I was doing because I assume someone else will fix it.			0.686	
When someone sends me a link, I open it without first verifying where it goes.			0.793	
I verify that my antivirus software has been regularly updating itself.				0.731
When browsing websites, I mouse over links to see where they go, before clicking them.			-0.368	0.439

I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.			0.701	
I do not change my passwords, unless I have to.		-0.606		
I use different passwords for different accounts that I have.		0.587		
I do not include special characters in my password if it's not required.		-0.694		
When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.		0.722		
I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon).		-0.357	0.562	
Eigen Values	1.156	1.556	1.972	3.785
Percentage of variance	11.07%	13.09%	13.8%	14.97%
Total variance	52.93%			

Note: Factor loadings <0.3 are suppressed

An overall moderate internal consistency was obtained for all the four outcome variables with Cronbach's alphas (α = 0.604) for SeBIS_DeviceSecurement, (α = 0.646) for SeBIS_PasswordGeneration, (α = 0.675) for SeBIS_ProactiveAwareness and (α = 0.749) for SeBIS_Updating subscales, with N=369.

Internal consistencies were also evaluated for all the predictor variable scales. Responses on all the predictor variable scales had moderate to excellent internal consistency: DOSPERT_Ethical (α = 0.802), DOSPERT_Financial (α =0.767), DOSPERT_Health/Safety (α = 0.748), DOSPERT_Social (α =0.624), GDMS_Rational (α = 0.767), GDMS_Intuitive (α = 0.78), GDMS_Dependent (α = 0.759), GDMS_Avoidant (α =0.91), GDMS_Spontaneous (α = 0.859), IPIP_Agreeableness (α = 0.804), IPIP_Conscientiousness (α = 0.857),

IPIP_Neuroticism (α = 0.873), IPIP_Openness (α = 0.803), IPIP_Extraversion (α = 0.868), IPIP_Risk-Avoidance (α = 0.89).

5.2. Descriptives

The survey sample includes students and faculty/staff from diverse roles, majors and employment duration but with less diverse age and citizenship. The majority of the sample is in the age group of 18-25 and are U.S. citizens. These will be considered when interpreting the results. Demographic data distribution of the sample is presented in Table 2.

Table 2: Demographic Data (N=369)

Demographic Factors	**Mean**	**SD**	**Groups**	**Percentages**
Age	31.47	15.31	18-25	57.7%
			26-35	11%
			36-45	9.3%
			46-55	9.3%
			56-65	8.7%
			65+	4.1%
Gender			Female	59.4%
			Male	40.6%
Role			Student	65.8%
			Faculty/Staff	34.2%
Majors (For students, n = 212)			Humanities	16%
			Business	17.7%
			Behavioral Sciences	29.1%
			Engineering	37.2%
Citizenship			U.S. Citizen	90.1%
			Non U.S. Citizen	9.9%
Employment Length (For faculty/staff, n=122)			0-5 yrs	40.2%
			6-10 yrs	15.4%
			11-20 yrs	25.6%
			20+ yrs	18.8%

Appendix D presents the means and standard deviations for all predictor and outcome variables. Step-wise multiple regression analysis is performed on the sets of predictor variables and outcome variables to test the hypotheses.

5.3. Multiple Regression Analysis

Multiple regression analysis was coducted with predictor variables, risk-taking preferences, decision-making styles, personality traits and demographics on the four outcome variables of online security behaviors, device securement, password generation, proactive awareness and updating. Only demographic factors of age, gender, role and citizenship are included in the regression model as major and employment length do not apply to the entire sample. Major is relevant only to the sub-sample of students and employment length only to the sub-sample of faculty/staff. The results are organized by outcome variable.

5.3.1. Device Securement

Ordinary Least Square (OLS) regressions were run on device securement as the outcome variable and risk-taking preferences, decision-making styles, personality traits and demographics as the predictor variables. Table 3 lists the standardized and unstandardized betas along with standard errors for the regression model.

There was no significant unique effect of any single kind of risk-taking preferences on users' security behavior of device securement. In decision-making styles, rational decision-making style ($\beta=0.164, p<0.01$) was a significant unique predictor. In personality traits, extraversion ($\beta=0.142, p<0.05$) was found to be a significant unique predictor. There was no significant unique effect of any

demographic factor on users' security behavior of device securement. Therefore, Hypothesis H1 (hypothesizing influence of risk-taking preferences on device securement) is not supported. Hypothesis H2a (hypothesizing the influence of rational decision-making style) is supported while the remaining H2 hypotheses are not supported. Hypothesis H3e (hypothesizing the influence of extraversion on device securement) is supported, while the remaining H3 set of hypotheses are not supported. Hypotheses H4 is not supported. Further mean differences across security behaviors are tested using ANOVA's in the next sections. Overall, the predictors in the regression model account for 5.2% of variance in users' security behaviors of device securement.

Table 3: Regression results for online security behavior of device securement

	Regression Coefficients		
Predictor Variable	**B**	**SE B**	**β**
Risk-Taking Preferences			
Ethical Risk Taking	0.043	0.073	0.051
Financial Risk Taking	-0.049	0.062	-0.058
Health/Safety Risk Taking	0.001	0.062	0.002
Social Risk Taking	0.009	0.059	0.009
Decision-Making Style			
Rational Decision Making	0.267	0.099	**0.164****
Intuitive Decision Making	-0.024	0.088	-0.017
Dependant Decision Making	-0.014	0.081	-0.01
Avoidant Decision Making	-0.065	0.066	-0.068
Spontaneous Decision Making	0.036	0.085	0.031
Personality Traits			
Agreeableness	0.095	0.107	0.056
Conscientiousness	0.027	0.102	0.019
Neuroticism	-0.044	0.081	-0.036
Openness	-0.069	0.091	-0.045
Extraversion	0.186	0.08	**0.142***
Risk Avoidance	0.011	0.081	0.01
Demographic Factors			
Age	-0.009	0.005	-0.154
Gender	0.027	0.106	0.014
Role	-0.1	0.155	-0.05
Citizenship	-0.27	0.159	-0.091
Adjusted R^2		0.052	

*p<0.05. **p<0.01. ***p<0.001.

5.3.2. Password Generation

OLS regressions were run on password generation as the outcome variable and risk-taking preferences, decision-making styles, personality traits and demographic factors as the predictor variables. Table 4 lists the standardized and unstandardized betas along with standard errors for the regression model.

Table 4: Regression results for online security behavior of password generation

	Regression Coefficients		
Predictor Variable	**B**	**SE B**	**β**
Risk-Taking Preferences			
Ethical Risk Taking	-0.02	0.06	-0.027
Financial Risk Taking	0.104	0.05	**0.141****
Health/Safety Risk Taking	-0.137	0.051	**-0.211***
Social Risk Taking	0.089	0.049	0.107
Decision-Making Style			
Rational Decision Making	0.016	0.081	0.011
Intuitive Decision Making	-0.061	0.072	-0.048
Dependant Decision Making	-0.093	0.066	-0.077
Avoidant Decision Making	-0.125	0.054	**-0.149***
Spontaneous Decision Making	-0.003	0.07	-0.003
Personality Traits			
Agreeableness	-0.043	0.087	-0.029
Conscientiousness	0.2	0.084	**0.166***
Neuroticism	-0.041	0.066	-0.038
Openness	-0.011	0.074	-0.008
Extraversion	0.122	0.066	0.106
Risk Avoidance	-0.045	0.067	-0.048
Demographic Factors			
Age	0.002	0.004	0.033
Gender	0.261	0.087	**0.157****
Role	-0.063	0.127	-0.037
Citizenship	0.074	0.13	0.029
Adjusted R^2		0.168	

*p<0.05. **p<0.01. ***p<0.001.

In risk-taking preferences, financial risk-taking ($\beta=0.141, p<0.01$) and health/safety risk-taking ($\beta=-0.211, p<0.05$) were found to be unique significant predictors. In decision-making styles, avoidant decision-making style ($\beta=-0.149, p<0.05$) was a significant unique predictor. In personality traits, conscientiousness ($\beta=0.166, p<0.05$) was found to be a significant unique predictor. In demographic factors, gender ($\beta=0.157, p<0.01$) was found to have a unique significant effect on users' online security behavior of password generation. Therefore, Hypothesis H1 (hypothesizing influence of risk-taking preferences on password generation) is supported for H1c. In addition, H1b was surprisingly found to be supported in the reverse direction. Hypothesis H2 (hypothesizing the influence of decision-making style on password generation) is supported for only H2d while the remaining H2 hypotheses are not supported. Hypothesis H3 (hypothesizing the influence of personality traits on password generation) is supported is supported only for H3b, while the remaining H3 set of hypotheses are not supported. Hypotheses H4b is supported for unique effect while others are not. Further mean differences across security behaviors are tested using ANOVA's in the next sections. Overall, the predictors in the regression model account for 16.8% of variance in users' security behaviors of device securement.

5.3.3. Proactive Awareness

OLS regressions were run on proactive awareness as the outcomes variable and risk-taking preferences, decision-making styles, personality traits and demographic factors as the predictor variables. Table 5 lists the standardized and unstandardized betas along with standard errors for the regression model.

Table 5: Regression results for online security behavior of proactive awareness

	Regression Coefficients		
Predictor Variable	**B**	**SE B**	**β**
Risk-Taking Preferences			
Ethical Risk Taking	-0.107	0.054	**-0.152***
Financial Risk Taking	0.007	0.046	0.009
Health/Safety Risk Taking	-0.084	0.046	-0.137
Social Risk Taking	0.022	0.044	0.027
Decision-Making Style			
Rational Decision Making	0.182	0.074	**0.135***
Intuitive Decision Making	-0.037	0.066	-0.031
Dependant Decision Making	-0.123	0.06	**-0.108***
Avoidant Decision Making	-0.124	0.049	**-0.157***
Spontaneous Decision Making	-0.056	0.063	-0.057
Personality Traits			
Agreeableness	-0.035	0.079	-0.025
Conscientiousness	-0.05	0.076	-0.044
Neuroticism	0.03	0.06	0.03
Openness	0.112	0.067	0.09
Extraversion	0.092	0.06	0.085
Risk Avoidance	-0.038	0.061	-0.043
Demographic Factors			
Age	0.002	0.004	0.047
Gender	0.212	0.079	**0.135****
Role	0.156	0.115	0.096
Citizenship	0.106	0.118	0.044
Adjusted R^2		0.228	

*p<0.05. **p<0.01. ***p<0.001.

In risk-taking preferences, ethical risk-taking (*β=-0.152, p<0.05*) was found to be a unique significant predictor. In decision-making styles, rational decision-making style (*β=-0.135, p<0.05*), dependent decision-making style (*β=-0.108, p<0.05*), and avoidant decision-making style (*β=-0.157, p<0.05*) were found to have significant unique effects on proactive awareness. There was no significant unique effect of any personality traits on users' security behavior of proactive awareness. In demographic factors, gender (*β=0.135, p<0.01*) was found to have a unique significant effect on users' online security behavior of proactive awareness. Therefore, Hypothesis H1 (hypothesizing influence of risk-taking preferences on proactive awareness) is

supported for H1a, while others are not supported. Hypothesis H2 (hypothesizing the influence of decision-making style on password generation) is supported for only H2a, H2c and H2d while the remaining H2 hypotheses are not supported. Hypothesis H3 (hypothesizing the influence of personality traits on password generation) is not supported. Hypotheses H4b is supported for unique effect while others are not. Further mean differences across security behaviors are tested using ANOVA's in the next sections. Overall, the predictors in the regression model account for 22.8% of variance in users' security behaviors of device securement.

5.3.4. Updating

OLS regressions were run on updating as the outcome variable and risk-taking preferences, decision-making styles, personality traits and demographic factors as the predictor variables. Table 6 lists the standardized and unstandardized betas along with standard errors for the regression model.

Table 6: Regression results for online security behavior of updating

	Regression Coefficients		
Predictor Variable	**B**	**SE B**	**β**
Risk-Taking Preferences			
Ethical Risk Taking	0.127	0.071	0.145
Financial Risk Taking	0.056	0.061	0.065
Health/Safety Risk Taking	-0.131	0.061	**-0.172***
Social Risk Taking	0.071	0.058	0.072
Decision-Making Style			
Rational Decision Making	0.256	0.098	**0.153****
Intuitive Decision Making	-0.14	0.087	-0.093
Dependant Decision Making	0.148	0.08	0.104
Avoidant Decision Making	-0.057	0.065	-0.058
Spontaneous Decision Making	0.294	0.084	**0.243*****
Personality Traits			
Agreeableness	-0.005	0.105	-0.003
Conscientiousness	0.256	0.101	**0.181***
Neuroticism	-0.035	0.079	-0.028
Openness	-0.16	0.089	-0.103

Extraversion	0.014	0.079	0.01
Risk Avoidance	0.103	0.08	0.092
Demographic Factors			
Age	0.009	0.005	0.144
Gender	0.264	0.104	**0.135***
Role	-0.077	0.152	-0.038
Citizenship	0.063	0.157	0.021
Adjusted R^2		0.126	

*p<0.05. **p<0.01. ***p<0.001.

In risk-taking preferences, health/safety risk-taking (*β=-0.172, p<0.05* was found to be a unique significant predictor. In decision-making styles, rational decision-making style (*β=0.153, p<0.01*) and spontaneous decision-making style (*β=0.243, p<0.001*) were found to have unique significant effects. In personality traits, conscientiousness (*β=0.181, p<0.05*) was found to be a significant unique predictor. In demographic factors, gender (*β=0.135, p<0.05*) was found to have a unique significant effect on users' online security behavior of password generation. Therefore, Hypothesis H1 (hypothesizing influence of risk-taking preferences on password generation) is supported for H1c. Hypothesis H2 (hypothesizing the influence of decision-making style on password generation) is supported for only H2a. In addition, H2e is supported in reverse direction, while the remaining hypotheses are not supported. Hypothesis H3 (hypothesizing the influence of personality traits on password generation) is supported only for H3b, while the remaining H3 set of hypotheses are not supported. Hypotheses H4b is supported for unique effect while others are not. Further mean differences across security behaviors are tested using ANOVA's in the next sections. Overall, the predictors in the regression model account for 12.6% of variance in users' security behaviors of device securement.

The overall significant effects of the predictors on the outcomes variables is summarized in Table 7:

Table 7: Summarizing the regression analysis coefficients

	Device Securement	**Password Generation**	**Proactive Awareness**	**Updating**
Ethical Risk Taking			-0.152*	
Financial Risk Taking		0.141*		
Health/Safety Risk Taking		-0.21**		-0.172*
Social Risk Taking				
Rational Decision Making	0.164**		0.135*	0.153**
Intuitive Decision Making				
Dependant Decision Making			-0.108*	
Avoidant Decision Making		-0.149*	-0.157*	
Spontaneous Decision Making				0.243***
Risk Avoidance				
Extraversion	0.142*			
Agreeableness				
Conscientiousness		0.166*		0.181*
Neuroticism				
Openness				
Age				
Gender		0.157**	0.135*	0.135*
Role				
Citizenship				

*p<0.05. **p<0.01. ***p<0.001.

It is important to note that the predictors were not consistently related to the four studied constructs of security behavior. For example, spontaneous decision-making was a strong predictor of the security behavior, updating, but was not associated with the other three outcome variables. The uniformity and diversity of the patterns of predictors on four outcomes variables and the possible underlying reasons for such patterns is discussed in the discussion section in detail.

ANOVA's along with post-hoc tests of Tukey HSD and Games-Howell were conducted to test research question 2, i.e. the mean differences of online security behaviors across demographics of age, gender, role, major, citizenship and employment length.

5.4. User Online Security Behavior by demographics

H4 was tested with a series of ANOVAs. Results show that user security behaviors differ significantly across the demographic factors age, gender, role and majors. There were no significant differences observed across the demographic factors of citizenship and employment length in the university. Another important finding is that the demographic factors, which were found to have significant differences, did not differ uniformly with all of the four outcome variables. The following sections explain the findings further.

5.4.1. Age

ANOVA findings for H4a show significant differences in security behaviors of password generation, proactive awareness and updating among the various age groups, but no significant differences in device securement were found. Table 8 shows the results of ANOVA organized by outcome variables.

Table 8: Mean differences in security behavior by Age

	Source	df	SS	MS	F
Device Securement	Between Groups	5	9.56	1.912	2.231
	Within Groups	337	288.818	0.857	
	Total	342	298.379		
Password Generation	Between Groups	5	11.457	2.291	**3.419****
	Within Groups	338	226.508	0.67	
	Total	343	237.966		

Proactive Awareness	Between Groups	5	25.798	5.16	**9.531*** **
	Within Groups	337	182.444	0.541	
	Total	342	208.243		
Updating	Between Groups	5	16.02	3.204	**3.554** **
	Within Groups	337	303.783	0.901	
	Total	342	319.802		

*p<0.05. **p<0.01. ***p<0.001.

For the outcome variable of password generation, which had significant differences among age groups (F (5,338) = 3.419, p<0.01), the age group of 18-25 had lower security behaviors compared to the age group of 46-55 (p<0.05). However, there were no significant differences found among other age groups.

For the outcome variable of proactive awareness, which had significant differences among age groups (F (5,337) = 9.531, p<0.001), the age group of 18-25 had significantly weaker proactive awareness compared to the age groups of 36-45 (p<0.05), 46-55 (p<0.05) and 56-65(p<0.01).

For the outcome variable of updating, which had significant differences among age groups (F (5,337) = 3.554, p<0.01), the age group of 18-25 had significantly weaker security behaviors compared to the age groups of 26-35 (p<0.05).

H4a, which states younger people have lower security behaviors, is thus supported, as age groups of 18-25 in comparison to older age groups had significantly lower security behaviors of password generation, proactive awareness and updating, though with no difference in device securement.

5.4.2. Gender

ANOVA findings for H4b show significant differences in security behaviors of password generation, proactive awareness and updating, but no significant differences in device securement by gender. Table 9 shows the results of ANOVA organized by outcome variables.

Table 9: Mean differences in security behavior by Gender

	Source	df	SS	MS	F
Device Securement	Between Groups	1	0.147	0.147	0.168
	Within Groups	341	298.232	0.875	
	Total	342	298.379		
Password Generation	Between Groups	1	9.565	9.565	**14.322*** **
	Within Groups	342	228.401	0.668	
	Total	343	237.966		
Proactive Awareness	Between Groups	1	3.92	3.92	**6.542***
	Within Groups	341	204.323	0.599	
	Total	342	208.243		
Updating	Between Groups	1	7.884	7.884	**8.619****
	Within Groups	341	311.919	0.915	
	Total	342	319.802		

*p<0.05. **p<0.01. ***p<0.001.

Females in comparison to males had lower security behaviors of password generation ($F(1,342) = 14.322$, $p<0.001$), proactive awareness ($F(1,341) = 6.542$, $p<0.05$), and updating ($F(1,341) = 8.619$, $p<0.01$). Thus, H4b is supported for security behaviors of password generation, proactive awareness and updating but not for device securement.

5.4.3. Role

ANOVA findings for H4c show significant differences in security behaviors of all four outcome variables of device securement, password generation, proactive

awareness and updating for students vs faculty/staff. Table 10 shows the results of ANOVA organized by outcome variables.

Table 10: Mean differences in security behavior by Role

	Source	df	SS	MS	F
Device Securement	Between Groups	1	4.3	4.3	**4.987***
	Within Groups	341	294.078	0.862	
	Total	342	298.379		
Password Generation	Between Groups	1	4.458	4.458	**6.529***
	Within Groups	342	233.508	0.683	
	Total	343	237.966		
Proactive Awareness	Between Groups	1	19.583	19.583	**35.396*****
	Within Groups	341	188.66	0.553	
	Total	342	208.243		
Updating	Between Groups	1	4.565	4.565	**4.938***
	Within Groups	341	315.237	0.924	
	Total	342	319.802		

*p<0.05. **p<0.01. ***p<0.001.

One-way ANOVA for testing the mean differences in security behavior by role showed significant differences for all of the four outcome variables of device securement ($F(1,341) = 4.987$, $p<0.05$), password generation ($F(1,341) = 6.529$, $p<0.05$), proactive awareness ($F(1,341) = 35.396$, $p<0.001$) and Updating ($F(1,341) = 4.938$, $p<0.05$). However, the division of role into student and faculty/staff would also have age as a factor, as age of faculty/staff would be much higher than students. To account for this, ANCOVA was run on outcome variables by role controlling for age. Table 11 shows the ANCOVA results organized by the outcome variables.

Table 11: ANCOVA on security behavior by Role controlled by Age

	Source	SS	df	MS	F
Device Securement	Age	4.269	1	4.269	5.009*
	Role	0.148	1	0.148	0.173
	Error	289.809	340	0.852	

Password Generation	Age	1.013	1	1.013	1.505
	Role	0.190	1	0.190	0.282
	Error	228.974	340	0.673	
Proactive Awareness	Age	1.829	1	1.829	3.329
	Role	2.591	1	2.591	**4.716***
	Error	186.83	340	0.550	
Updating	Age	2.278	1	2.278	2.475
	Role	0.009	1	0.009	0.010
	Error	312.959	340	0.92	

After controlling for age, there were significant differences by role only for proactive awareness ($F(1,1,340) = 4.716$, $p<0.01$). Faculty/staff were noted to have high security behaviors of proactive awareness ($p<0.05$). H4c, which states students would have higher security behavior than faculty/staff, was thus supported partly, as the faculty/staff group was observed to have better proactive awareness.

5.4.4. Majors

ANOVA findings for H4d show significant differences in security behaviors for device securement and password generation. Table 12 shows the results of ANOVA organized by outcome variables.

Table 12: Mean differences in security behavior by Major

		df	SS	MS	F
Device Securement	Between Groups	3	9.501	2.375	**2.802***
	Within Groups	212	178.872	0.848	
	Total	215	188.372		
Password Generation	Between Groups	3	8.418	2.104	**3.378***
	Within Groups	212	131.441	0.623	
	Total	215	139.859		
Proactive Awareness	Between Groups	3	2.507	0.627	1.092
	Within Groups	213	121.057	0.574	
	Total	215	123.564		
Updating	Between Groups	3	7.31	1.827	1.903
	Within Groups	213	202.657	0.96	
	Total	215	209.967		

*p<0.05. **p<0.01. ***p<0.001.

For the outcome variable of device securement, which had significant differences among majors ($F(3,212) = 2.802$, $p<0.01$), engineering majors had higher security behavior compared to humanities ($p<0.05$). However, there were no significant differences found among other majors of behavioral sciences and business.

For the outcome variable of password generation, which had significant differences among majors ($F(3,212) = 3.378$, $p<0.01$), engineering majors had higher security behaviors compared to humanities ($p<0.05$). However, there were no significant differences found among the other majors of behavioral sciences and business. H4d, that engineering and technical majors have better security behavior as compared to non-technical majors, is supported for behaviors of device securement and password generation.

5.4.5. Citizenship

ANOVA findings for H4e were non-significant for all outcome variables. Table 13 shows the results of ANOVA organized by outcome variables.

Table 13: Mean differences in security behavior by Citizenship

		df	SS	MS	F
Device Securement	Between Groups	1	4.096	0.683	0.779
	Within Groups	341	294.283	0.876	
	Total	342	298.379		
Password Generation	Between Groups	1	1.261	0.21	0.299
	Within Groups	341	236.704	0.702	
	Total	343	237.966		
Proactive Awareness	Between Groups	1	6.679	1.113	1.856
	Within Groups	341	201.563	0.6	
	Total	342	208.243		
Updating	Between Groups	1	3.32	0.553	0.587

	Within Groups	341	316.483	0.942
	Total	342	319.802	

The distribution of sample between U.S. Citizens and Non-U.S. Citizens category is in ratio of 9:1, and hence would have resulted in not identifying the differences between the two groups. Thus, H4e is not supported.

5.4.6. Employment Length in the university

ANOVA findings for H4f were non-significant differences for all four outcome variables. Table 14 shows the results of ANOVA organized by outcome variables.

Table 14: Mean differences in security behavior by Employment Length

		df	SS	MS	F
Device Securement	Between Groups	3	6.828	1.366	1.509
	Within Groups	119	105.914	0.905	
	Total	122	112.742		
Password Generation	Between Groups	3	4.357	0.871	1.113
	Within Groups	119	91.59	0.783	
	Total	122	95.947		
Proactive Awareness	Between Groups	3	3.613	0.723	1.523
	Within Groups	119	55.506	0.474	
	Total	122	59.119		
Updating	Between Groups	3	5.71	1.142	1.588
	Within Groups	119	84.113	0.719	
	Total	122	89.823		

Hypothesis H4f that security behaviors increase with the employment length in the university is not supported.

Further, non-response analysis was performed to test for the presence of a non-response bias in the survey data. The next section presents the results of the non-response analysis.

5.5. Non-Response Analysis

Demographics of age, gender, role, major and citizenship were considered as factors for non-response analysis. Non-response bias of age was tested using t-test to compare the average ages of response and non-response groups. Chi-square tests were performed to check for non-response bias in gender, role, major and citizenship. Following is the summary of the statistical test results:

- Average age of respondents (M = 31.47, SD = 15.3) in comparison to average of of non-respondents (M = 28.53, SD = 13.57) was significantly higher ($t(4266) = 3.941$, $p<0.01$). Therefore, respondents were slightly older than non-respondents.
- There was a significant non-response bias introduced by gender (X^2 (1, N= 4353) = 33.87, $p<0.01$). Respondents were more likely to be females.
- There was a significant non-response bias introduced by role ($X^2(1, N= 4353) = 15.767$, $p<0.01$). Faculty/Staff were more likely to respond than students.
- There was no significant non-response bias introduced with the demographic factor of major in the students sub-sample ($X^2(1, N= 1683) = 3.846$, $p=0.279$).
- There was a significant non-response bias introduced by citizenship (X^2 (1, N= 4353) = 4.861, $p<0.05$). Respondents were more likely to be U.S. Citizens.
- There was no significant difference $t(315) = 0.226$, $p = 0.763$) in the average employment length of respondents (M = 11.52, SD = 10.551) in comparison to average employment length of non-respondents (M = 11.79, SD = 10.482).

Overall, there was found to be a significant non-response bias in the demographic factors of age, gender, role and citizenship. Hence, the findings from the survey are subject to a possible non-response bias.

5.6. Interview Analysis

Descriptive open content coding was used to analyze the transcribed interviews and the observation forms. Focusing on the individual's phishing victimization and security practices, the following five problem areas were identified:

- **Gap in self risk-taking vs. researcher rating (lack of risk awareness):** There is a significant gap between the interviewee's assessment of the amount of risk they take and the interviewer's assessment. Self risk-taking is the self-rating given by the interviewees when asked to rate themselves on the risk they take online on a scale on 1 to 7. Researcher rating is the risk-taking rating given to each of the interviewees by the researchers based on their responses to computer and internet security practices and awareness of risks. There was a clear indication of a lack of risk awareness that was seen in the interviews, which accounted for the difference in these ratings.

- **Heavy reliance on local IT staff and lack of sense of responsibility:** In four of the seven interviews, there was a clear identification that the university members, in specific faculty/staff, who rely on the IT staff completely to account for their online security practices. Questions on their updating practices revealed that there is a lack of a sense of responsibility from the participant's end to secure themselves online. Instead, they see it as the job of the IT staff associated with the college.

- **Minimal understanding of expected cybersecurity behavior:** Consistent with Leach (2003), one of the key factors that influenced user security behaviors is the users' understanding of what behaviors are expected from them as part of the university, i.e. having knowledge of the values, policies, standards and procedures in the organization. In most of the interviews, the users indicated that they did not understand these.

- **Cybersecurity not a priority:** For five of the seven interviewees, cybersecurity was not a priority. The other jobs were given higher priority, and cybersecurity was viewed as a task for which no time could be spared.

- **Lack of a standard IT system for security reporting and ineffective outreach:** Many interviewees considered the IT division highly decentralized and lacking standard procedures for security reporting. They also did not know how to report security compromises

Table 15 lists supporting quotes that relate to the above-defined problem areas or gaps identified.

Table 15: Identified problem areas affecting security of the organization

Security Problem	Supporting Quotes and explanations
Gap in self risk-taking vs. researcher rating (Lack of risk awareness)	**High risk-taking self rating(On a scale from 1-7): 4-** "Maybe a 3.-4 I mean, I'm aware that just by going online you're exposing yourself to a certain amount of risk , and the balance is a risk; being shut off from everything." p. 6: "I am very careful about how I use my university assigned email address." "…My email is highly customized." (Interviewee#2)

	Interviewee doesn't download unnecessary things; doesn't click on links hastily, uses PayPal to make transactions; uses ProtectMyID service and checks reports, purchases security patches if required **Researcher rating: low- moderate risk-taking** vs **Low risk-taking selfrating:** 1 - "Social media, I don't do any". "The people in the chemistry IT mgt very well have suggested changing the password, uh, but I could just go back and forth between our grand-children's names and numbers." (Interviewee#3) **Researcher rating: moderate-high risk-taking**
Heavy reliance on local IT staff and lack of sense of responsibility	"If Sean tells me to do something, I do it." "If IT tells me to do something, I do it. Otherwise, it's possible, but I don't think I could care less." "I really don't. I mean, you guys..I mean, IT has a job to do, they do their job." (Interviewee#1) There were a few things that came from the IT group here, and I called Caedmon, and I said 'Hey, I've got this thing, and is it okay?" p. 9 "What I would do again is get in touch with Caedmon and if I noticed say greater incidents of things that appeared to be non-legitimate. But I don't install things myself. I'll call him and say, 'Do we need to install something? but I would have them do it." (Interviewee#3) High reliance on IT person for installing and updating anti-virus.
Minimal understanding of expected cybersecurity behavior	"Is this something I need to pay attention to?" "Do we need to install something? If so, I would have them do it." (Interviewee#7)
Cybersecurity not a priority	"I don't have time for this. Like, and you can tell people like, I do not have time for one more change...." Recalled mid-year switch to new course management system. "I do not want any more changes of stuff like this right now. Like, I don't have time for this. I do not have time." "...I'm an educated person. I obviously, like all these people are, and we know what we should be doing, and I know my colleagues, some of them are probably much better at it than I am, but I'm just like...'I don't know. That's like one more thing I need to do and figure out.' And I just don't have time." (Interviewee#7) "I do not care about this other stuff" "I just want it to work." (Interviewee#1)

	The above quotes from the interviewees indicated that their other jobs take priority and they don't have time to spare for cybersecurity.
Lack of standard IT system for security reporting and ineffective outreach	"I would have no idea how to report an issue. Just because of the email that was sent out that said, if you get this email let us know at this number, but, if that email hadn't gone out I dont think I would know who to contact because, to be honest, the system at this university is extremely confusing to me. School has its own IT, university has its IT. And sometimes, I contact the university IT about something and they're like, "No, you need to go to your school. So, I get really confused" (Interviewee#6) "sometimes the university, from what I recall, sent out an email to give us a heads up when something's, um, going around. I didn't think it was important So, maybe if that email had like, and maybe it was marked high importance, that would be helpful if it was. So those are the only kinda emails that I recall seeing. " (Interviewee#6)

Recommendations and possible solutions based on the above identified problem areas are discussed in detail in Section 6.

6. Discussion

This section presents a deeper interpretation of the results by providing implications for theory and for practice (security messaging). Toward the end of this section, general strategies or solutions for the problem areas identified through interview analysis are discussed.

6.1. Device Securement

In line with previous literature, risk-taking preferences were not found to have any relationship with the online security behavior of device securement. This reinforces that risk-taking is not an important factor that influences the user security behavior of securing devices. Previous research has found that people who engage in better security behaviors of device securement are less likely to have avoidant decision-making style (Egelman et al., 2015). However, this study did not find any relation between avoidant decision-making style and online security behavior of device securement in the regression model, indicating that avoidant decision-making style is not a unique predictor over the other predictor variables. Moreover, the rational decision-making style was a significant predictor. This suggests that people who engage in better security practices with device securement are likely to evaluate the decision of locking their device or using a PIN. Since only 5% of the variance in the outcome variable was explained by the predictor variables, there are other factors that need to be evaluated to identify the individual differences that influence this behavior. This study also extends previous research by looking at personality traits and demographic factors that influence the online security behavior of device securement. People who are more extraverted tend to have better security practices of updating.

When tested for the differences by demographic factors, engineering majors were found to have higher online security behavior of device securement in comparison to humanities. Table 16 consolidates the results of hypothesis testing on the security behavior outcome, device securement.

Table 16: Results of hypothesis testing for device securement

Predictor Variables (Hypothesis)	**Device Securement (Hypothesis Testing)**	**Result**
Risk-Taking Preferences		
Ethical (H1a)	t(346) = 0.594, ns	Not supported
Financial (H1b)	t(346) = -0.799, ns	Not supported
Health/Safety (H1c)	t(346) = 0.019, ns	Not supported
Social (H1e)	t(346) = 0.143, ns	Not supported
Decision-Making Styles		
Rational (H2a)	**t(346) = 2.691, p<0.01**	**Supported**
Intuitive (H2b)	t(346) = -0.278, ns	Not supported
Dependant (H2c)	t(346) = -0.174, ns	Not supported
Avoidant (H2d)	t(346) = -0.976, ns	Not supported
Spontaneous (H2e)	t(346) = 0.427, ns	Not supported
Personality Traits		
Agreeableness (H3a)	t(346) = 0.889, ns	Not supported
Conscientiousness (H3b)	t(346) = 0.262, ns	Not supported
Neuroticism (H3c)	t(346) = -0.541, ns	Not supported
Openness (H3d)	t(346) = -0.757, ns	Not supported
Extraversion (H3e)	**t(346) = 2.315, p<0.05**	**Supported**
Risk Avoidance (H3f)	t(346) = 0.131, ns	Not supported
Demographics		
Age (H4a)	F(5,337) = 2.231, ns	Not supported
Gender (H4b)	F(1,341) = 0.168, ns	Not supported
Role (H4c)	F(1,340) = 0.173, ns	Not supported
Major (H4d)	**F(3,212) = 2.802, p<0.05**	**Supported**
Citizenship (H4e)	F(1,341) = 0.779, ns	Not supported
Employment Length (H4f)	F(3,119) = 1.509, ns	Not supported

6.2. Password Generation

Previous research has found correlations between engagement in better practices of password generation and rational and avoidant decision making styles. However, in this study, only avoidant decision-making style was found to be a significant factor. This implies that users' are less likely to evaluate their decision of choosing strong

passwords or reusing passwords in a systematic way. On the other hand, the internal consistency for outcome variable of password generation on SeBIS scale was found to be moderate. Hence this finding needs to be further evaluated with better measurement techniques.

In previous literature, individuals who are willing to take more ethical risks were found to engage in weaker security behaviors while users who take higher social risks were found to engage in better security behaviors (Egelman et al., 2015). In this study, while there were no significant correlations between ethical risk-taking and password generation, significant positive correlations were found with financial risk-taking, while negative correlation was found with health/safety risk-taking. This suggests that people who are willing to take higher financial risks tend to have better password generation practices, suggesting that they see a need for creating strong passwords and not reusing them. Also, people who care about their health/safety tend to have better security behaviors of password generation.

The predictors in the regression model explained close to 17% of the variance in the outcome variable. These results suggest security messages that aim to promote better security practices of password generation could include examples of the benefits of stronger passwords and reduced reuse of passwords in explaining the benefits they offer to investment or gambling accounts, while pointing to threats that could occur to health/safety when weak passwords are used.

In accordance with the earlier findings, although the demographics of age and major did not have unique effects in the regression model, ANOVA findings suggest

that younger people and women are more likely reuse passwords (Shay et al., 2010), women and those age 18-25 reported weaker security around password generation. On exploring additional demographics, individuals in engineering majors tend to have better password generation practices in comparison to humanities majors. Table 17 consolidates the results of hypothesis testing on security behavior outcome, password generation.

Table 17: Results of hypothesis testing for password generation

Predictor Variables (Hypothesis)	**Password Generation (Hypothesis Testing)**	**Result**
Risk-Taking Preferences		
Ethical (H1a)	t(346) = -0.342, ns	Not supported
Financial (H1b)	**t(346) = 2.053, p<0.05**	**Supported**
Health/Safety (H1c)	**t(346) = -2.688, p<0.05**	**Supported**
Social (H1e)	t(346) = 1.833, p<0.05	Supported
Decision-Making Styles		
Rational (H2a)	t(346) = 0.192, ns	Not supported
Intuitive (H2b)	t(346) = -0.844, ns	Not supported
Dependant (H2c)	t(346) = -1.407, ns	Not supported
Avoidant (H2d)	**t(346) = -2.293, p<0.01**	**Supported**
Spontaneous (H2e)	t(346) = -0.044, ns	Not supported
Personality Traits		
Agreeableness (H3a)	t(346) = -0.486, ns	Not supported
Conscientiousness (H3b)	**t(346) = 2.382, p<0.05**	**Supported**
Neuroticism (H3c)	t(346) = -0.618, ns	Not supported
Openness (H3d)	t(346) = -0.146, ns	Not supported
Extraversion (H3e)	t(346) = 1.855, ns	Not supported
Risk Avoidance (H3f)	t(346) = -0.679, ns	Not supported
Demographics		
Age (H4a)	**F(5,337) = 3.419, p<0.01**	**Supported**
Gender (H4b)	**F(1,341) = 14.332, p<0.001**	**Supported**
Role (H4c)	F(1,340) = 0.282, ns	Not supported
Major (H4d)	**F(3,212) = 3.378, p<0.05**	**Supported**
Citizenship (H4e)	F(1,341) = 0.299, ns	Not supported
Employment Length (H4f)	F(3,119) = 1.113, ns	Not supported

6.3. Proactive Awareness

Previous research has found correlations between engagement in better practices of proactive awareness to rational, avoidant and dependent decision-making styles. Also, individuals who are willing to take more ethical and health/safety risks were associated with weaker security behaviors (Egelman et al., 2015). This study's findings concur with the previous findings and do not have any further deviations, suggesting that people who are likely to engage in better password generation practices are not likely to procrastinate or depend on other factors to insure their security. Further, with addition of personality traits, there were no significant correlations in the model. Like the password generation measure, proactive awareness was found to have moderate internal consistency. Hence these results need to be further evaluated. The predictors in the regression model explain 23% of the variance in proactive awareness. Therefore, security messaging should draw attention to ethical and health/safety risks that could occur with lower compliance.

Again, though the demographic factors of age and role was not found to have a unique influence on proactive awareness, ANOVA findings suggest that women and those age 18-25 reported significantly weaker security behaviors of proactive awareness, suggesting that these groups pay lesser attention to contextual cues such as the URL bar or other browser indicators. This is consistent with the literature on the demographics of age and gender and phishing susceptibility (Sheng et al., 2010). When tested for role in the university, the faculty/staff were found to have higher proactive awareness, even after controlling for age. With regards to educational background, earlier research has found business, education and liberal arts students to be more vulnerable to spear phishing attacks than technology and science students

(Darwish et al., 2012). However, this study did not find any significant differences for both the groups of students and faculty/staff on the outcome variable of proactive awareness. As mentioned earlier, this finding should be evaluated further owing to the moderate internal consistency of the outcome variable obtained on SeBIS scale. Table 18 consolidates the results of hypothesis testing on security behavior outcome, proactive awareness.

Table 18: Results of hypothesis testing for proactive awareness

Predictor Variables (Hypothesis)	**Proactive Awareness (Hypothesis Testing)**	**Result**
Risk-Taking Preferences		
Ethical (H1a)	**t(346) = -1.977, p<0.05**	**Supported**
Financial (H1b)	t(346) = 0.143, ns	Not supported
Health/Safety (H1c)	**t(346) = -1.822, p<0.05**	**Supported**
Social (H1e)	t(346) = 0.488, ns	Not supported
Decision-Making Styles		
Rational (H2a)	**t(346) = 2.464, p<0.05**	**Supported**
Intuitive (H2b)	t(346) = -0.569, ns	Not supported
Dependant (H2c)	**t(346) = -2.046, p<0.05**	**Supported**
Avoidant (H2d)	**t(346) = -2.507, p<0.01**	**Supported**
Spontaneous (H2e)	t(346) = -0.885, ns	Not supported
Personality Traits		
Agreeableness (H3a)	t(346) = -0.446, ns	Not supported
Conscientiousness (H3b)	t(346) = -0.658, ns	Not supported
Neuroticism (H3c)	t(346) = 0.498, ns	Not supported
Openness (H3d)	t(346) = 1.661, ns	Not supported
Extraversion (H3e)	t(346) = 1.540, ns	Not supported
Risk Avoidance (H3f)	t(346) = -0.632, ns	Not supported
Demographics		
Age (H4a)	**F(5,337) = 9.531, p<0.001**	**Supported**
Gender (H4b)	**F(1,341) = 6.542, p<0.05**	**Supported**
Role (H4c)	**F(1,340) = 4.716, p<0.05**	**Supported**
Major (H4d)	F(3,212) = 1.092, ns	Not supported
Citizenship (H4e)	F(1,341) = 1.856, ns	Not supported
Employment Length (H4f)	F(3,119) = 1.523, ns	Not supported

6.4. Updating

Previous research has found positive correlations between engagement in better practices of updating to rational, avoidant and spontaneous decision-making styles. Moreover, individuals who are willing to take more ethical and health/safety risks were associated with lower security behavior (Egelman et al., 2015). This study's findings differed significantly from the earlier findings. While health/safety risk-taking preferences still remained significant predictors of updating security behaviors, there was no relationship between ethical risk-taking preferences and updating. Since the earlier studies have only explored correlations and not tested for unique influence of the factors on updating, it can be inferred that ethical risk-taking does not uniquely predict users' security behaviors of keeping software up-to-date.

With decision-making styles, while rational, avoidant and decision-making styles correlated significantly before the addition of personality traits, the effect of avoidant decision-making style was suppressed with conscientiousness and risk-avoidance personality traits significantly predicted the security behaviors of updating. This suggests that people who have better security behaviors of updating tend to be risk-averse rather than procrastinating. Since conscientiousness is a significant predictor, in addition to the emphasis on risk-taking and decision-making, messages emphasizing policy adherence and standards may be more effective.

When tested for the effect of demographics, although age was not found to have a unique effect in the regression model, ANOVA findings suggest that women and those age 18-25 were less likely to keep software up-to-date. This was in line

with the other three outcome variables. Table 19 consolidates the results of hypothesis testing on security behavior outcome, proactive awareness.

Table 19: Results of hypothesis testing for updating

Predictor Variables (Hypothesis)	**Updating (Hypothesis Testing)**	**Result**
Risk-Taking Preferences		
Ethical (H1a)	t(346) = 1.774, p<0.05	Not Supported
Financial (H1b)	t(346) = 0.925, ns	Not supported
Health/Safety (H1c)	**t(346) = -2.139, p<0.05**	**Supported**
Social (H1e)	t(346) = 1.215, ns	Not supported
Decision-Making Styles		
Rational (H2a)	**t(346) = 2.614, p<0.05**	**Supported**
Intuitive (H2b)	t(346) = -1.612, ns	Not supported
Dependant (H2c)	t(346) = 1.855, p<0.05	Supported
Avoidant (H2d)	t(346) = -0.876, p<0.01	Supported
Spontaneous (H2e)	**t(346) = 3.520, ns**	**Not supported**
Personality Traits		
Agreeableness (H3a)	t(346) = -0.047, ns	Not supported
Conscientiousness (H3b)	**t(346) = 2.543, ns**	**Not supported**
Neuroticism (H3c)	t(346) = -0.438, ns	Not supported
Openness (H3d)	t(346) = -1.790, ns	Not supported
Extraversion (H3e)	t(346) = 0.176, ns	Not supported
Risk Avoidance (H3f)	t(346) = 1.281, ns	Not supported
Demographics		
Age (H4a)	**F(5,337) = 3.554, p<0.01**	**Supported**
Gender (H4b)	**F(1,341) = 8.619, p<0.01**	**Supported**
Role (H4c)	F(1,340) = 0.010, ns	Supported
Major (H4d)	F(3,212) = 1.903, ns	Not supported
Citizenship (H4e)	F(1,341) = 0.587, ns	Not supported
Employment Length (H4f)	F(3,119) = 1.588, ns	Not supported

As discussed in the above sections, the results varied by the type of security behavior. For example, the predictor variable, financial risk-taking was associated with the security behavior of password generation, but not with other security behaviors of device securement, proactive awareness and updating. An overview of the results from the statistical testing of the entire hypothesis from the research model is presented in Table 20.

Table 20: Overall summary of the results testing the research model

Predictor Variables	Device Securement	Password Generation	Proactive Awareness	Updating
Risk-Taking Preferences				
Ethical	t(346) = 0.594, ns	t(346) = -0.342, ns	**t(346) = -1.977, p<0.05**	t(346) = 1.505, ns
Financial	t(346) = -0.799, ns	**t(346) = 2.053, p<0.05**	t(346) = 0.143, ns	t(346) = 1.046, ns
Health/Safety	t(346) = 0.019, ns	**t(346) = -2.688, p<0.05**	t(346) = -1.822, p<0.05	**t(346) = -2.471, p<0.05**
Social	t(346) = 0.143, ns	t(346) = 1.833, p<0.05	t(346) = 0.488, ns	t(346) = 1.530, ns
Decision-Making Styles				
Rational	**t(346) = 2.691, p<0.01**	t(346) = 0.192, ns	**t(346) = 2.464, p<0.05**	**t(346) = 2.478, p<0.05**
Intuitive	t(346) = -0.278, ns	t(346) = -0.844, ns	t(346) = -0.569, ns	t(346) = -1.774, ns
Dependant	t(346) = -0.174, ns	t(346) = -1.407, ns	**t(346) = -2.046, p<0.05**	t(346) = 1.742, ns
Avoidant	t(346) = -0.976, ns	**t(346) = -2.293, p<0.01**	**t(346) = -2.507, p<0.01**	t(346) = -1.050, ns
Spontaneous	t(346) = 0.427, ns	t(346) = -0.044, ns	t(346) = -0.885, ns	**t(346) = 3.971, p<0.001**
Personality Traits				
Agreeableness	t(346) = 0.889, ns	t(346) = -0.486, ns	t(346) = -0.446, ns	t(346) = -0.317, ns
Conscientiousness	t(346) = 0.262, ns	**t(346) = 2.382, p<0.05**	t(346) = -0.658, ns	**t(346) = 2.497, p<0.05**
Neuroticism	t(346) = -0.541, ns	t(346) = -0.618, ns	t(346) = 0.498, ns	t(346) = -1.110, ns
Openness	t(346) = -0.757, ns	t(346) = -0.146, ns	t(346) = 1.661, ns	t(346) = -1.754, ns
Extraversion	**t(346) = 2.315, p<0.05**	t(346) = 1.855, ns	t(346) = 1.540, ns	t(346) = -0.101, ns
Risk Avoidance	t(346) = 0.131, ns	t(346) = -0.679, ns	t(346) = -0.632, ns	**t(346) = 2.204, p<0.05**
Demographics				
Age	F(5,337) = 2.231, ns	**F(5,337) = 3.419, p<0.01**	**F(5,337) = 9.531, p<0.001**	**F(5,337) = 3.554, p<0.01**
Gender	F(1,341) = 0.168, ns	**F(1,341) = 14.332,p<0.001**	**F(1,341) = 6.542, p<0.05**	**F(1,341) = 8.619, p<0.01**
Role	F(1,340) = 0.173, ns	F(1,340) = 0.282, ns	**F(1,340) = 4.716, p<0.05**	F(1,340) = 0.010, ns
Major	**F(3,212) = 2.802, p<0.05**	**F(3,212) = 3.378, p<0.05**	F(3,212) = 1.092, ns	F(3,212) = 1.903, ns
Citizenship	F(1,341) =	F(1,341) =	F(1,341) =	F(1,341) =

Employment Length	0.779, ns F(3,119) = 1.509, ns	0.299, ns F(3,119) = 1.113, ns	1.856, ns F(3,119) = 1.523, ns	0.587, ns F(3,119) = 1.588, ns

ns-not significant

6.5. Recommendations

Based on the findings from the survey and interviews, the following recommendations for better organizational cybersecurity are provided.

- **Identify and emphasize different strategies to promote different security behaviors.** Since the predictor variables did not have uniform effects over all the outcome variables of security behaviors, security messaging must be tailored to the kind of security behavior that is being promoted.

- **Increase risk awareness and security training, and security messaging.** There was a clear identified gap between the users' perception of their risk-taking and what is suggested from their responses to Internet security practices. This indicates a lack of risk awareness and hence emphasizes the need for training. Also, when asked about the training/awareness exposure, no participant referred to educational materials from the university. The only exposure they had was either from their earlier environments or general security advice that is available online. In addition, when asked for suggestions into what could have helped, a majority pointed to services that would keep reminding them regularly of the risks. Participants also felt a need for training to be precise and to the point. An interesting suggestion was having security advice delivered through an alert system to keep the users aware of any alarming incidents. Campus alert systems are emergency

messaging services that distribute time-sensitive alerts via voice, email, and text.

- **Increase efforts to improve users' understanding of what behaviors are expected from them.** In addition to the training that has been earlier emphasized, there is a clear lack of understanding of university policies, standards and expectations of cybersecurity behavior.

- **Review university policies to regulate, automate, or mandate regular software updates.** Through the interviews, a theme that was found in a majority of the cases was high reliance on IT staff in the college and department units to update software.

- **Emphasize the importance of cybersecurity, the interruption that could occur to regular tasks, and the loss of time in recovering from such situations.** Cybersecurity was observed to have a lower priority in comparison to the regular tasks and responsibilities of most interview participants.

- **Adopt better promotional and awareness practices to achieve higher compliance with organizational security.** Participants emphasized their difficulty in security reporting. They cited two reasons. The first relates to the organization's structure being both bureaucratic (having a centralized organization delivering services on a university-wide bases) and multi-divisional (in which individual academic or business units operate their own departmental information technology structures to provide services to their respective constituents). Discovering the appropriate point of contact in such a structure was noted as a frustration. The second is the lack of information

about and promotion of a centralized reporting service for security matters. For example, ‘spam@umd.edu’ exists as a service to report spams and spurious emails. However, there is not enough outreach to the university community to notify students, faculty, and staff about this service.

7. Conclusion

In this section, we offer a summary, research limitations and suggestions for future research.

7.1. Summary

In view of employees being the weakest link in organization cybersecurity, the present study findings contribute towards the goal of turning this weakest link into a strong asset, by determining the most common characteristics of the individuals that are likely to engage in better security practices. Identification of characteristics of individuals who pose the biggest security risks for organizations can help organizations tailor their security messaging and awareness programs to ensure that vulnerabilities created by these "riskier" individuals are addressed. The predictor variables of risk-taking preferences, decision-making styles and personality traits accounted for about 5-23% of the variance that is associated with online security behaviors, indicating that the findings can be employed to achieve higher organization security compliance. The study results also emphasized the variations in the security messages or nudges that ought to be given to promote different security behaviors. However, there is a need to explore further individual differences and other factors to achieve better predictability. The interviews with the phishing attack victims exposed the gaps and vulnerabilities in the organization as a whole, which when addressed would contribute to improved organizational security.

7.2. Limitations

There are several limitations to this study. First, the response rate was low (~9% to the surveys), and there was evidence of a non-response bias. Since the organization that is studied is a university, the sample was unusually young students and hence it was difficult to tease out differences in the sample. This resulted in lower power of the multivariate tests analyzed separately for the sub-groups of student and faculty/staff. Also, the results of this study might not hold true for other organizations in different sectors that have a more diversified user base.

Second, since the nature of the data collection was through an online survey, the responses to the security behavior indicate the self-reported data about the user behaviors, and hence, could be biased and may not reflect users' actual behavior. The research model should be further tested in a lab experiment for validity.

Third, since only seven interviews could be conducted, the findings and identified problem areas might not reflect the population at large. More interviews need to be conducted until saturation is achieved.

Fourth, there could be possible threats to internal and external validity of the results. A threat to internal validity could be extraneous variables like awareness of security policies of the organization and training, which were not a part of the research model. A threat to external validity could be the low response rate on the surveys and interviews. Due to the possibility of a non-response bias, the sample may differ from the population.

7.3. Future Research

The findings from the interviews identify the need to conduct further research in the identified gap areas. Measures like awareness of security policies of the organization and training, which were not a part of this study, should be considered in the future. Based on the findings of the study, interventions should be developed, and suggestions of security messaging should be developed and tested through further research, to determine what strategies would better promote organizational security.

8. Appendix

8.1. Appendix A – Survey Instrument

Project Title	Risk Assessment of Phishing Victims at a University
Purpose of the Study	This research is being conducted by Dr. Michel Cukier at the University of Maryland, College Park. We are inviting you to participate in this research project because you have been selected as part of a random sample of members of the university. The purpose of this research is to provide the university with information on computer usage behavior from students, faculty and staff.
Procedures	The procedures involve completing a personality survey, a series of questions about your behavior online and offline, and demographic information. You will complete the survey from your personal computer. The survey should take less than 20 minutes to complete. After completing the survey, you will be entered in a drawing for 50 $10 gift cards. All prize winnings are considered taxable income; gift card winners are responsible for any taxes assessed on the $10 prize. Example Questions: Rate each item on a scale of 1 to 5, with 1 being Strongly Disagree, 3 being Neutral, and 5 being Strongly Agree. *I have frequent mood swings* *I make quick decisions.*
Potential Risks and Discomforts	There is little direct risk in participating in this survey. There is a small risk of embarrassment, as you will be asked questions about sensitive topics such as your drinking habits and sexual history. All information will be kept confidential and secured. You do not have to answer any question that makes you feel uncomfortable. You may quit the survey at any time or skip any question with which you are uncomfortable, for any reason. Your participation in this research is completely voluntary. You may choose not to take part at all.
Potential Benefits	This survey will help researchers and campus policy makers better understand the factors that make faculty, staff, and students vulnerable to phishing attacks. We hope that the university will be able to use this research to create better strategies and educational materials aimed at keeping our community safe from cyber threats. Your responses are a valuable component in helping enhance campus security and shape information technology policy.

Confidentiality	Any potential loss of confidentiality will be minimized by taking all appropriate measures to protect your data. If we write a report or article about this research paper, your identity will be protected to the maximum extent possible. All results will be reported in aggregate, with no personal identifiers attached that could facilitate identification. A hard copy of your consent form will be saved in a secure location. Your information may be shared with representatives of the University of Maryland, College Park or governmental authorities if you or someone else is in danger or if we are required to do so by law.
Right to Withdraw and Questions	Your participation in this research is completely voluntary. You may choose not to take part at all. If you decide to participate in this research, you may stop participating at any time. If you decide not to participate in this study or if you stop participating at any time, you will not be penalized or lose any benefits to which you otherwise qualify. Your academic standing or professional position will not be affected by your decision to terminate participation. If you decide to stop taking part in the study, if you have questions, concerns, or complaints, or if you need to report an injury related to the research, please contact the investigator: Dr. Michel Cukier Phone: 3013142804 Address: 3149 AV Williams, University of Maryland Email: mcukier@umd.edu
Participant Rights	If you have questions about your rights as a research participant or wish to report a research-related injury, please contact: **University of Maryland College Park** **Institutional Review Board Office** **1204 Marie Mount Hall** **College Park, Maryland, 20742** **E-mail: irb@umd.edu** **Telephone: 301-405-0678** This research has been reviewed according to the University of Maryland, College Park IRB procedures for research involving human subjects.
Statement of Consent	Your consent indicates that you are at least 18 years of age; you have read this consent form or have had it read to you; your questions have been answered to your satisfaction and you voluntarily agree to participate in this research study. You are advised to print a copy of the consent form for your records. If you agree to participate, please click "I Consent" below.
Consent	**[I CONSENT]**

Section 1: Personality Traits (IPIP)

Please indicate to what extent each of the following statements applies to you.

(1) Very Inaccurate, (2) Moderately Inaccurate, (3) Neither Inaccurate nor Accurate, (4) Moderately Accurate, (5) Very Accurate.

Extraversion

1. I feel comfortable around people.
2. I make friends easily.
3. I am skilled in handling social situations.
4. I am the life of the party.
5. I know how to captivate people.
6. I have little to say.
7. I keep in the background.
8. I would describe my experiences as somewhat dull.
9. I don't like to draw attention to myself.
10. I don't talk a lot.

Agreeableness

11. I have a good word for everyone.
12. I believe that others have good intentions.
13. I respect others.
14. I accept people as they are.
15. I make people feel at ease.
16. I have a sharp tongue.
17. I cut others to pieces.
18. I suspect hidden motives in others.
19. I get back at others.
20. I insult people.

Conscientiousness

21. I am always prepared.
22. I pay attention to details.
23. I get chores done right away.
24. I carry out my plans.
25. I make plans and stick to them.
26. I waste my time.
27. I find it difficult to get down to work.
28. I do just enough work to get by.
29. I don't see things through.
30. I shirk my duties.

Neuroticism

31. I often feel blue.
32. I dislike myself.
33. I am often down in the dumps.
34. I have frequent mood swings.
35. I panic easily.
36. I rarely get irritated.
37. I seldom feel blue.
38. I feel comfortable with myself.
39. I am not easily bothered by things.

40. I am very pleased with myself.

Openness to experience

41. I believe in the importance of art.
42. I have a vivid imagination.
43. I tend to vote for liberal political candidates.
44. I carry the conversation to a higher level.
45. I enjoy hearing new ideas.
46. I am not interested in abstract ideas.
47. I do not like art.
48. I avoid philosophical discussions.
49. I do not enjoy going to art museums.
50. I tend to vote for conservative political candidates.

Risk-Avoidance

51. I would never go hang-gliding or bungee jumping.
52. I would never make a high-risk investment.
53. I avoid dangerous situations.
54. I seek danger.
55. I am willing to try anything once.
56. I do dangerous things.
57. I enjoy being reckless.
58. I seek adventure.
59. I take risks.
60. I do crazy things.

Section 2: Decision-Making Style (GDMS)

Please indicate to what extent you agree or disagree with each of the following statements, according to the five-point scale below ranging from Strongly Disagree to Strongly Agree.

(1) Strongly Disagree, (2) Disagree, (3) Neutral, (4) Agree, (5) Strongly Agree.

1. When I make decisions, I tend to rely on my intuition.*(Intuitive)*
2. I rarely make important decisions without consulting other people. *(Dependent)*
3. When I make a decision, it is more important for me to feel the decision is right than to have a rational reason for it. *(Intuitive)*
4. I double check my information sources to be sure I have the right facts before making decisions. *(Rational)*
5. I use the advice of other people in making my important decisions. *(Dependent)*
6. I put off making decisions because thinking about them makes me uneasy. *(Avoidant)*
7. I make decisions in a logical and systematic way. *(Rational)*
8. When making decisions I do what feels natural at the moment. *(Spontaneous)*
9. I generally make snap decisions. *(Spontaneous)*
10. I like to have someone steer me in the right direction when I am faced with important decisions. *(Dependent)*
11. My decision making requires careful thought. *(Rational)*
12. When making a decision, I trust my inner feelings and reactions. *(Intuitive)*

13. When making a decision, I consider various options in terms of a specified goal. *(Rational)*
14. I avoid making important decisions until the pressure is on. *(Avoidant)*
15. I often make impulsive decisions. *(Spontaneous)*
16. When making decisions, I rely upon my instincts. *(Intuitive)*
17. I generally make decisions that feel right to me. *(Intuitive)*
18. I often need the assistance of other people when making important decisions. *(Dependent)*
19. I postpone decision making whenever possible. *(Avoidant)*
20. I often make decisions on the spur of the moment. *(Spontaneous)*
21. I often put off making important decisions. *(Avoidant)*
22. If I have the support of others, it is easier for me to make important decisions. *(Dependent)*
23. I generally make important decisions at the last minute. *(Avoidant)*
24. I make quick decisions. *(Spontaneous)*
25. I explore all of my options before making a decision. *(Rational)*

Section 3: Online Security Behaviors (SeBIS)

Please indicate your response to the following questions based on how they apply to you.

(1) Never, (2) Rarely, (3) Sometimes, (4) Often, (5) Always.

1. When I'm prompted about a software update, I install it right away. *(Updating)*
2. I try to make sure that the programs I use are up-to-date. *(Updating)*
3. I manually lock my computer screen when I step away from it. *(Device Securement)*
4. I set my computer screen to automatically lock if I don't use it for a prolonged period of time. *(Device Securement)*
5. I use a PIN or passcode to unlock my mobile phone. *(Device Securement)*
6. I use a password/passcode to unlock my laptop or tablet. *(Device Securement)*
7. If I discover a security problem, I continue what I was doing because I assume someone else will fix it. *(Proactive Awareness)*
8. When someone sends me a link, I open it without first verifying where it goes. *(Proactive Awareness)*
9. I verify that my anti-virus software has been regularly updating itself. *(Updating)*
10. When browsing websites, I mouseover links to see where they go, before clicking them. *(Proactive Awareness)*
11. I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar. *(Proactive Awareness)*
12. I do not change my passwords, unless I have to. *(Password Generation)*
13. I use different passwords for different accounts that I have. *(Password Generation)*
14. I do not include special characters in my password if it's not required. *(Password Generation)*
15. When I create a new online account, I try to use a password that goes beyond the site's minimum requirements. *(Password Generation)*

16. I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon). *(Proactive Awareness)*

Section 4: Risk-Taking Preferences (DOSPERT)

For each of the following statements, please indicate the likelihood that you would engage in the described activity or behavior if you were to find yourself in that situation.

(1) Extremely Unlikely, (2) Moderately Unlikely, (3) Somewhat Unlikely, (4) Not Sure, (5) Somewhat Likely, (6) Moderately Likely, (7) Extremely Likely.

1. Admitting that your tastes are different from those of a friend. *(Social)*
2. Going camping in the wilderness. *(Recreational)*
3. Betting a day's income at the horse races. *(Financial)*
4. Investing 10% of your annual income in a moderate growth mutual fund. *(Financial)*
5. Drinking heavily at a social function. *(Health/Safety)*
6. Taking some questionable deductions on your income tax return. *(Ethical)*
7. Disagreeing with an authority figure on a major issue. *(Social)*
8. Betting a day's income at a high-stake poker game.
9. Having an affair with a married person. *(Ethical)*
10. Passing off somebody else's work as your own. *(Ethical)*
11. Going down a ski run that is beyond your ability. *(Recreational)*
12. Investing 5% of your annual income in a very speculative stock. *(Financial)*
13. Going whitewater rafting at high water in the spring. *(Recreational)*
14. Betting a day's income on the outcome of a sporting event. *(Financial)*
15. Engaging in unprotected sex. *(Health/Safety)*
16. Revealing a friend's secret to someone else. *(Ethical)*
17. Driving a car without wearing a seat belt. *(Health/Safety)*
18. Investing 10% of your annual income in a new business venture. *(Financial)*
19. Taking a skydiving class. *(Recreational)*
20. Riding a motorcycle without a helmet. *(Health/Safety)*
21. Choosing a career that you truly enjoy over a more prestigious one. *(Social)*
22. Speaking your mind about an unpopular issue in a meeting at work. *(Social)*
23. Sunbathing without sunscreen. *(Health/Safety)*
24. Bungee jumping off a tall bridge. *(Recreational)*
25. Piloting a small plane. *(Recreational)*
26. Walking home alone at night in an unsafe area of town. *(Health/Safety)*
27. Moving to a city far away from your extended family. *(Social)*
28. Starting a new career in your mid-thirties. *(Social)*
29. Leaving your young children alone at home while running an errand. *(Ethical)*
30. Not returning a wallet you found that contains $200. *(Ethical)*

Section 5: Demographic questions

We would like you to tell us about your background so that we can review our practices and develop new strategies to improve online security for all our community members.

1. What is your gender?

- ( ) Male
- ( ) Female
- ( ) Trans male/trans man
- ( ) Trans female/trans woman
- ( ) Gender queer/gender non-conforming
- ( ) Different identity
- ( ) Decline to respond

2. What is your age? (respondents should be 18 or over) (pick one)

- ( ) 18 – 24
- ( ) 25 – 34
- ( ) 35 – 44
- ( ) 45 – 54
- ( ) 55 – 64
- ( ) 65+

3. What is your ethnicity? (check all that apply)

   Are you of Hispanic, Latino, or Spanish origin?

   ( ) No, not of Hispanic, Latino, or Spanish origin
   ( ) Yes, Mexican, Mexican American, Chicano
   ( ) Yes, Puerto Rican
   ( ) Yes, Cuban
   ( ) Yes, another Hispanic, Latino, or Spanish origin
   ( ) Unavailable/Unknown
   ( ) Decline to respond

4. What is your race? (check all that apply)

- ( ) American Indian/Alaska Native
- ( ) Asian
- ( ) Black or African American
- ( ) Native Hawaiian/Other Pacific Islander
- ( ) White
- ( ) Some other race
- ( ) Decline to respond
- ( ) Unavailable/Unknown

5. What is your highest level of education? (pick one)

- ( ) Some high school
- ( ) High school graduate
- ( ) Some college/Currently in college (undergraduate)
- ( ) College graduate

- ( ) Some graduate/Currently in graduate or professional program
- ( ) Graduate degree or professional program completed
- ( ) Other _____

6. Are you: (pick one)
- ( ) Not currently a student (skip 6a)
- ( ) A student in an undergraduate program
- ( ) A student in a graduate program
- ( ) A student in some other type of program? Specify: _____

- 6.a. What is your undergraduate major or name of your graduate program? _____

7. Employment status: are you currently? (check all that apply)
- ( ) Employed for wages
- ( ) Self-employed
- ( ) Out of work and looking for work
- ( ) Out of work but not currently looking for work
- ( ) A homemaker
- ( ) A student
- ( ) Military
- ( ) Retired
- ( ) Unable to work

8. What is your marital status? (pick one)
( ) Single, never married
( ) Married or domestic partnership
( ) Widowed
( ) Divorced
( ) Separated

9. Are you a citizen of the United States? (pick one)
- ( ) Yes, born in the United States (skip 9a)
- ( ) Yes, born in Puerto Rico, Guam, the U. S. Virgin Islands, or Northern Marianas.
- ( ) Yes, born abroad of US citizen parent or parents
- ( ) Yes, US citizen by naturalization. Print year of naturalization: __ __ __ __
- ( ) No

- **9.a. When did you come to live in the United States?** (If you came to live in the US more than once, print latest year) __ __ __ __

10. Do you speak a language other than English at home?
- ( ) Yes (please answer 10a and 10b)
- ( ) No (skip 10a and 10b)

- 10.a. What language(s) do you speak at home?
  _____

- 10.b. How well do you understand/read written English? (pick one)
- ( ) Beginner
- ( ) Intermediate
- ( ) Advanced
- ( ) Native proficiency

11. Rate your level of experience with computers/Internet: (pick one)
- ( ) None
- ( ) Beginner
- ( ) Intermediate
- ( ) Advanced
- ( ) Expert

11. Do you use any of the following types of computers? (check all that apply)

a. Desktop ____ yes ____ no
b. Laptop ____ yes ____ no
c. Tablet or other portable wireless computer ____ yes ____ no
d. Some other type of computer ____ yes ____ no

12. How many hours do you average online per day? (pick one)

( ) 0-2
( ) 3-4
( ) 5-6
( ) 7-8
( ) 9 or more

8.2. Appendix B – Interview Protocol & Observation Form

1. Briefly, please introduce yourself and your role at the university.

2. You were selected to participate in this interview because your email account was compromised in a phishing incident. Can you please share with us what you remember from the incident?

3. Division of Information Technology records retained a copy of the phishing email from the incident. [Provide the message to the participant.] Please take a look and comment on anything else you recall from the incident. Tell me what you notice about this email. If you received this today, what would you notice about it?

4. Do you recall how the incident was brought to your attention? Did you notice something wrong with your account or was someone in contact with you? Tell us about that, please. And, what loss, if any, did you experience as a result of the incident (time, data)?

5. What tools, if any, do you use in your email program to filter messages, report junk mail, etc. to manage your inbox?

6. Have you been exposed to any awareness/education efforts about phishing? Please share what you recall about them—content, sources in which you remember seeing information?

7. A 2-part question:
Following the incident, how, if at all, did your behavior change?
Following the education effort, how, if at all, did your behavior change?
(If the participant identifies a change, follow up with: Has the change been sustained?

8. On a scale of 1 to 7, with 1 being low and 7 being high, give yourself a rating on the level of risk you take online, and comment on why you rate yourself at that level.

9. Software patches and operating system updates are provided by software companies to guard against exploits of vulnerabilities that could lead to a compromise of security or identity. Please tell us about your regularity of installing updates and updating your anti-virus software.

10. When a friend posts a link on social media, what precautions, if any, do you employ when deciding whether or not to click on it?

11. If someone sends you a personalized message with a link (through email, social media, etc.), how do you decide whether or not to open the link? Does your relationship with the sender matter?

12. Were you familiar with the concept of social engineering before the phishing attack or this interview? What other attacks do you know of?

13. If you had to give recommendations to your friends regarding how to avoid being phished, what would you tell them?

14. What ideas do you have about how phishing incidents could be minimized?

15. What might an effective campaign to prevent phishing victimization look like?

16. Are we talking about what is important to talk about?

17. Is there anything we didn't ask you that you would like to mention?

Observation Form

- What were the main issues or themes that struck you in the interview?
- What visible displays of intensity did you see in the interviewee? (Be as specific as possible, if you can recall what was being talked about at the time, note it.)
- Note anything else that struck you as salient, interesting, illuminating or important in the interview.
- What new (or remaining) questions do you now have for the next interview or others in the organization?
- Other observations

8.3. Appendix C – Correlation matrix between predictor and outcomes

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Extraversion	1	.245**	.244**	-.345**	.205**	-.235**	0.027	.184**	0.069	-.218**	.116*	-0.057	0.072	.126*	.150**	.151**
Agreeableness	.245**	1	.402**	-.393**	.291**	.131*	.169**	-0.065	0.038	-.319**	-.246**	-.382**	-.265**	-.295**	-.117*	-0.008
Conscientiousness	.244**	.402**	1	-.422**	.211**	.248**	.330**	-0.002	-0.088	-.573**	-.245**	-.353**	-.272**	-.298**	-.245**	-0.036
Neuroticism	-.345**	-.393**	-.422**	1	-.122*	0.076	-.158**	-0.015	0.098	.381**	0.099	.123*	-0.04	0.083	-0.082	-0.042
Openness	.205**	.291**	.211**	-.122*	1	0.034	.222**	0.09	0.052	-.189**	-0.09	-.231**	-0.094	-.199**	-0.058	.313**
Risk-avoidance	-.235**	.131*	.248**	0.076	0.034	1	.164**	-.217**	0.011	-.108*	-.422**	-.388**	-.430**	-.610**	-.750**	-.291**
Rational Decision-Making	0.027	.169**	.330**	-.158**	.222**	.164**	1	-0.011	.211**	-.147**	-.325**	-.209**	-.138**	-.183**	-0.039	.114*
Intuitive Decision-Making	.184**	-0.065	-0.002	-0.015	0.09	-.217**	-0.011	1	.131*	0.078	.464**	.128*	.162**	.218**	.109*	.147**
Dependent Decision-Making	0.069	0.038	-0.088	0.098	0.052	0.011	.211**	.131*	1	.261**	0.022	.105*	0.005	0.047	0.042	-0.082
Avoidant Decision-Making	-.218**	-.319**	-.573**	.381**	-.189**	-.108*	-.147**	0.078	.261**	1	.304**	.344**	.245**	.249**	.157**	-0.058
Spontaneous Decision-Making	.116*	-.246**	-.245**	0.099	-0.09	-.422**	-.325**	.464**	0.022	.304**	1	.427**	.356**	.445**	.288**	.132*
Ethical Risk-Taking	-0.057	-.382**	-.353**	.123*	-.231**	-.388**	-.209**	.128*	.105*	.344**	.427**	1	.626**	.680**	.393**	.138**
Financial Risk-Taking	0.072	-.265**	-.272**	-0.04	-0.094	-.430**	-.138**	.162**	0.005	.245**	.356**	.626**	1	.513**	.458**	.257**
Health/Safety Risk-Taking	.126*	-.295**	-.298**	0.083	-.199**	-.610**	-.183**	.218**	0.047	.249**	.445**	.680**	.513**	1	.615**	.243**
Recreational Risk-Taking	.150**	-.117*	-.245**	-0.082	-0.058	-.750**	-0.039	.109*	0.042	.157**	.288**	.393**	.458**	.615**	1	.319**
Social Risk-Taking	.151**	-0.008	-0.036	-0.042	.313**	-.291**	.114*	.147**	-0.082	-0.058	.132*	.138**	.257**	.243**	.319**	1

Device Securement	.174**	.105*	.116*	-.117*	0.024	-0.072	.168**	0.028	0.052	-.114*	-0.023	0	-0.013	0.041	.154**	0.039
Password Generation	.158**	.135**	.284**	-.260**	.121*	0.014	.110*	-0.047	-.144**	-.319**	-.107*	-.154**	0.03	-.172**	-0.017	.133*
Proactive Awareness	0.086	.183**	.230**	-.157**	.225**	.161**	.217**	-.110*	-.153**	-.319**	-.254**	-.378**	-.208**	-.324**	-.104*	0.062
Updating	0.036	0.048	.200**	-.133*	-0.014	0.096	.180**	-0.011	0.079	-0.095	0.066	0.026	0.045	-0.086	-0.021	0.048

**** Correlation is significant at the 0.01 level (2-tailed).**

*** Correlation is significant at the 0.05 level (2-tailed).**

8.4. Appendix D – Means and standard deviations for all continuous predictors and outcomes

(N=369)

Variable	Mean	Standard Deviation
Ethical Risk Taking	2.1385	1.101
Financial Risk Taking	2.4947	1.11401
Health/Safety Risk Taking	2.7466	1.25721
Social Risk Taking	4.7529	0.9795
Rational Decision Making	3.9912	0.57561
Intuitive Decision Making	3.5122	0.64298
Dependant Decision Making	3.5526	0.67649
Avoidant Decision Making	2.6927	0.976
Spontaneous Decision Making	2.637	0.79317
Risk Avoidance	3.1544	0.85564
Extraversion	3.4298	0.71444
Agreeableness	3.9091	0.5532
Conscientiousness	3.7065	0.68045
Neuroticism	2.4045	0.76585
Openness	3.9468	0.61765
Age	31.47	15.3
Employment Length	11.52	10.551

9. References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Anschuetz, C. (2015). The Weakest Link Is Your Strongest Security Asset. Retrieved from http://blogs.wsj.com/cio/2015/02/26/the-weakest-link-is-your-strongest-security-asset/

Anti-Phishing Working Group. (2016). Phishing Activity Trends Report 4th Quarter 2015. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q4_2015.pdf

Appelt, K. C., Milch, K. F., Handgraaf, M. J., & Weber, E. U. (2011). The decision making individual differences inventory and guidelines for the study of individual differences in judgment and decision-making research. *Judgment and Decision Making, 6*(3), 252-262.

Arachchilage, N. A., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304-312.

Arnett, J. J. (1996). Sensation seeking, aggressiveness, and adolescent reckless behavior. *Personality and Individual Differences, 20*(6), 693-702.

Blythe, J., Camp, J., & Garg, V. (2011). Targeted risk communication for computer security. *Proceedings of the 16th International Conference on Intelligent User Interfaces - IUI '11,* 295-298.

Boyle, G. J., Matthews, G., & Saklofske, D. H. (2008). *The SAGE handbook of personality theory and assessment*. Los Angeles, CA: SAGE Publications.

Charness, G., Gneezy, U., & Imas, A. (2013). Experimental methods: Eliciting risk preferences. *Journal of Economic Behavior & Organization, 87*, 43-51.

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

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. *Proceedings of the Anti-phishing Working Groups 2nd Annual ECrime Researchers Summit on - ECrime '07,* 37-44.

Egelman, S., & Peer, E. (2015). Predicting privacy and security attitudes. *SIGCAS Comput. Soc. ACM SIGCAS Computers and Society, 45*(1), 22-28.

Egelman, S., & Peer, E. (2015). Scaling the Security Wall. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15,* 2873-2882.

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. *Proceedings of the 22nd International Conference on World Wide Web - WWW '13 Companion,* 737-744.

Interpol. (2015). Interpol cyber experts meeting aims to advise on global strategy. Retrieved from http://www.interpol.int/News-and-media/News/2015/N2015-209

John, O. P., Robinson, R. W., & Pervin, L. A. (2011). *Handbook of personality: Theory and research*. New York: Guilford.

Leach, J. (2003). Improving user security behaviour. *Computers & Security, 22*(8), 685-692.

Mohebzada, J. G., Zarka, A. E., Bhojani, A. H., & Darwish, A. (2012). Phishing in a university community: Two large scale phishing experiments. *2012 International Conference on Innovations in Information Technology (IIT),* 249-254.

Ng, B., Kankanhalli, A., & Xu, Y. (. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.

Pattinson, M. R., & Anderson, G. (2007). How well are information risks being communicated to your computer end-users? *Info Mngmnt & Comp Security Information Management & Computer Security, 15*(5), 362-371.

Pattinson, M., Jerram, C., Parsons, K., Mccormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Info Mngmnt & Comp Security Information Management & Computer Security, 20*(1), 18-28.

Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. (2009). A Personality Based Model for Determining Susceptibility to Phishing Attacks. *Decision sciences Institute,* 285-296.

PricewaterhouseCoopers. Global State of Information Security® Survey 2016. (2015). Retrieved from http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Anonymity, Privacy, and Security

Online. Retrieved from http://pewinternet.org/Reports/2013/Anonymity-online.aspx

Scott, S. G., & Bruce, R. A. (1995). Decision-Making Style: The Development and Assessment of a New Measure. *Educational and Psychological Measurement, 55*(5), 818-831.

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., . . . Cranor, L. F. (2010). Encountering stronger password requirements. *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10,* 2.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10,* 373-382.

Soto, C. J., John, O. P., Gosling, S. D., & Potter, J. (2011). Age differences in personality traits from 10 to 65: Big Five domains and facets in a large cross-sectional sample. *Journal of Personality and Social Psychology, 100*(2), 330-348.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

TAMIR, D. (2013). FBI Warns of Increase in Spear-Phishing Attacks. Retrieved from https://securityintelligence.com/fbi-warns-increase-spear-phishing-attacks/

Thunholm, P. (2004). Decision-making style: Habit, style or both? *Personality and Individual Differences, 36*(4), 931-944.

US-CERT. (2013). Avoiding social engineering and phishing attacks. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-014