Spring 2017

Impact of framing and priming on users' behavior in cybersecurity

Kavya Sharma

IMPACT OF FRAMING AND PRIMING ON USERS' BEHAVIOR IN CYBERSECURITY

by

KAVYA SHARMA

A THESIS

Presented to the Faculty of the Graduate School of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE IN INFORMATION SCIENCE & TECHNOLOGY

2017

Approved by

Dr. Fiona Fui-Hoon Nah
Dr. Keng Siau
Dr. Richard Hall

ABSTRACT

This research examines the impact of framing and priming on users' behavior (i.e., action) in a cybersecurity setting. It also examines perceptual outcomes (i.e., confidence, perceived severity, perceived susceptibility, trust, and fear) associated with the users' cybersecurity action. The research draws on prospect theory in the behavioral economics literature and instance-based learning theory in the education literature to generate the hypotheses for the research. A between-subject experimental design (N=129) was used. The results suggest that priming users to cybersecurity risks reduces their risk-taking behavior associated with cybersecurity whereas negative framing of messages associated with cybersecurity has no significant effect on users' behavior. The results also suggest that users who had taken a risk adverse cybersecurity action exhibited greater confidence associated with their action, perceived greater severity associated with cybersecurity risks, perceived lower susceptibility of their computer to cybersecurity risks, and perceived lower trust in the download link they had encountered in the experiment. This research suggests that priming is an effective way to reduce cybersecurity risks faced by users.

Keywords: Cybersecurity, Framing, Priming, Users' Behavior, Confidence, Perceived Severity, Perceived Susceptibility, Trust, and Fear

ACKNOWLEDGMENTS

I would like to express my gratitude to my advisor, Dr. Fiona Fui-Hoon Nah, for the endless support, guidance, and encouragement. Her patience and knowledge has been exceptional. She helped me from the start till the end of this research and provided me with all the knowledge required to complete my research as well as assisted me with data analysis. It has been a great learning experience under her supervision. Also, it has been a gratifying experience to become one of her co-authors for a paper published in the Lecture Notes in Computer Science.

I would like to express my gratitude to the rest of my thesis committee members, Dr. Keng Siau and Dr. Richard Hall, for their support and feedback that assisted me to further improve and enhance this research. I would like to thank Dr. Wei Jiang for his help in having his students participate as pilot subjects for the study. I would also like to thank Dr. Chevy Fang, Mr. Nick Oswald and Ms. Carla Bates for allowing me to recruit subjects for the experiment in their classes.

I would like to thank my fellow research student, Samuel Smith, for providing his insights on how to proceed with simulation of the system and helping me with conducting the experimental study. I would also like to express my gratitude to all the Laboratory of Information Technology and Evaluation (LITE) students for helping me in setting up the lab sessions for conducting the experimental study.

Finally, I would like to thank my husband, my family and all my friends for having faith in me and encouraging me throughout my master's degree program.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

1. INTRODUCTION

Information technology corporations are greatly reliant on the usage of information systems for managing, communicating and storing data. In order to keep data secured in computer systems, it is necessary to protect the privacy, reliability and asset accessibility of these systems. However, there has been an increasing number of security related issues due to the rise in organizational dependency on computer systems (Kankanhalli, Teo, Tan, & Wei, 2003). In a CSI/FBI survey, majority of the respondents indicated that their organization faced information systems related security issues (Gordon, Loeb, Lucyshyn, & Richardson, 2006). Thus, it is crucial for organizations to defend themselves from cybersecurity risks. USA Department of Homeland Security refers to cybersecurity in "National Strategy to Secure Cyberspace" as sustaining the effective working of the organization that maintains critical data (DHS, 2003).

According to a report by IBM, more than 95% of the security occurrences in IBM were attributed to 'human errors' (IBM Corporation, 2014). An exceedingly propelled security framework comprising of firewalls might not be efficient at ensuring an organization's cyberspace security due to unintentional users' security behavior (Whitten & Tygar, 1999). Users play a vital role in identification and prevention of cybersecurity threats (Stanton, Mastrangelo, Stam, & Jolton, 2004). For instance, they must choose whether to install anti-virus software on their computer to shield it from viruses, download documents from anonymous sources, or provide personal credit card information for online transactions. Such choices include actions that could bring about different negative outcomes (e.g., loss of information, lower PC performance or damage

to a PC's hard drive). Therefore, there has been a shift toward studying user behavior in cybersecurity.

According to a cyber behavior decision model proposed by Aytes and Connolly (2004), people settle on a decision to either take part in protected or perilous cyber behavior. Aytes and Conolly's (2004) decision model states that users' cyber behavior is driven by views of the value of protected and risky practices and the outcomes of each. The model shows how the knowledge of prior cybersecurity related issues, one's relevant views on cybersecurity, and one's hazard attitudes can impact cybersecurity decision-making (Aytes & Connolly, 2004).

An imperative aspect of user behavior in cybersecurity is how users access and retort to goal-framed security messages that are intended to convince users to either impede or enhance their information security stance (Hong, 2012). The way in which the data exhibited to a user is framed has intermittently been recognized as a prime factor that affects user behavior. Users' security behavior plays a significant role in attaining cybersecurity (McNeese, et al., 2012).

In this research, a laboratory experiment was conducted to assess the impact of message framing and priming on users' behavior in cybersecurity. Specifically, we are interested in studying whether negatively framed security messages and the presence of priming lead users to take risk adverse actions.

This thesis is organized as follows. First, the literature review is presented which is followed by the theoretical foundation and the hypotheses. Next, the research methodology is described, after which the findings are presented and discussed. Finally, the limitations and directions for future research are also highlighted.

2. LITERATURE REVIEW

2.1. USERS' BEHAVIOR IN CYBERSECURITY

There exist various techniques for addressing cybersecurity, such as the technical framework for implementing security procedures and additional socio-technical methods of cybersecurity. In this literature review, we will focus on empirical studies that are related to factors affecting user behavior in information systems security. Users are the weakest target towards cybersecurity related threats (Siponen, 2000) and many researchers have studied the reasons for users' security responses and conduct (Lebek, Uffen, Breitner, Neumann, & Hohler, 2013).

A study that uses Protection Motivation Theory (PMT) has indicated that self-efficacy can predict secure behavior of customers (LaRose, Rifon, & Enbody, 2008). Based on the survey study by Woon et al. (2005), the perceived outcomes that influence end-users' cybersecurity actions are perceived severity, response cost, perceived susceptibility and self-efficacy (Woon, Tan, & Low, 2005). Pahnila et al. (2007) used various other features such as rewards, habits, sanctions, and information quality in order to study their effects on user behavior in cybersecurity (Pahnila, Siponen, & Mahmood, 2007).

The efficacy of coping response affects behavioral intents of the end-user in a positive manner for implementing suggested compliance behavior (Maddux & Rogers, 1983). Researchers studied the effect of fear appeal on security behavior of users under a high-risk environment for reducing the security threats using suggested instructions. Although having a fear appeal helps in persuading the user security behavior to follow the suggested instructions for risk mitigation, its effect is not consistent among all users.

Further, the effect of fear appeal on user security behavior depends on self-efficacy, gravity of the risk, and social impact (Johnston & Warkentin, 2010).

Several studies in information systems security suggest that though the prior knowledge of risks and suitable reactions is required to improve user security-related behavior, it is not enough (Lee & Kozar, 2005; Stanton, Stam, Mastrangelo, & Jolton, 2005; Sasse, Brostoff, & Weirich, 2001). It is essential to find the drivers of user behavior in cybersecurity in various situations and the ways to mitigate cybersecurity risks taken by users. Organizational cybersecurity continues to be adversely influenced by user security behavior. Hence, we have a long way to go in studying and analyzing the user factors leading to unfavorable security behavior in cybersecurity.

2.2. LITERATURE REVIEW ON MESSAGE FRAMING

Various researchers have utilized prospect theory to evaluate the impact of positively vs. negatively framed messages on users' behavior (Aaker & Lee, 2001; Shiv, Edell, & Payne, 2004). Prospect theory explains the procedure of decision-making that comprises a framing and an assessment stage. Even though positively vs. negatively framed messages may communicate the same information, the way a message is framed can impact the decision making process and outcomes of an individual (Tversky & Kahneman, 1986). Amidst the assessment stage, users assess choices by partly taking into account their individual values and outcomes in terms of whether a choice is seen to be an advantage or a disadvantage. The concept of loss aversion in prospect theory illustrates that users are more likely to react more to losses as compared to gains. Messages that accentuate the adverse results of an option are seen as possible damages to

which users are likely to maintain a greater distance as compared to the messages that underline the constructive results (Tversky & Kahneman, 1984).

Message framing includes underlining either the constructive facets of choosing an option, or the adverse facets of not choosing the option (Aaker & Lee, 2001). Protection Motivation Theory (PMT) has, to a great extent, been connected to health and natural settings to figure out which promotional messages adequately spur a man to make a move when confronted with a risk (for instance anti-smoking messages in the wellbeing context (Pechmann, Zhao, Goldberg, & Reibling, 2003) and water preservation messages in the eco-friendly context (Obermiller, 1995)).

The impact of message framing has been researched from both the financial and socio psychological standpoints in a diversity of decision-making perspectives, such as funds and societal predicaments (Brewer & Kramer, 1986). Researchers have studied the impact of message framing on various reliant variables covering intents (Block & Keller, 1995), idealness of messages, perceived prominence (Aaker & Lee, 2001) and threat awareness (Lee & Aaker, 2004). Users' behavioral intentions in cybersecurity can be further swayed by the usage of suitable messaging (LaRose, Rifon, & Enbody, 2008).

2.3. LITERATURE REVIEW ON PRIMING

If security threats are known to the individual in advance, then prior beliefs are formed by the individual regarding the severity of the security threats (Johnston & Warkentin, 2010; Workman, Bommer, & Straub, 2008; LaRose, Rifon, & Enbody, 2008). At the point when individuals get away from an approaching catastrophe by coincidence, they have encountered a "near miss." A near miss is an event where a risky or lethal effect could have happened, but it didn't happen (Dillon & Tinsley, 2008). According to

Tinsley et al. (2012), near miss is of two types, resilient near miss (that did not happen) and vulnerable near miss (debacle that almost occurred).

According to the disaster literature, user behavior is influenced by near miss or hit events. When individuals assess the danger of some unsafe occasions to be low, they are probably not going to take part in mitigation events. Moreover, any potential harm from previous debacles has been reported to considerably impact user perceptions of future hazards and to persuade more defensive conduct (Dillon, Tinsley, & Cronin, 2011). Having information of an experience of a hit encounter, including harmful effects in the past, would upsurge feelings of helplessness, and would lead the individuals to opt for a safer option.

When encountering an imminent risk, individuals ought to evaluate the risk, which is in fact an element of the likelihood of the incident happening and the damage that results from the incident if that happens (Kaplan & Garrick, 1981). Such evaluations utilize the current data, but individuals also incorporate any prior knowledge or information about the incident into their assessment of the hazard (Fishbein & Ajzen, 2010). This concept is explained in the subjective expected utility (SEU) model. Despite the fact that the SEU model gives a solid foundation for portraying how individuals choose to react to hazards, previous research has demonstrated that the model components can differ on the basis of the attributes of the condition (i.e., the same individual can opt for the safer option in one situation or can choose the risky option in another situation) (Fox & Tversky, 1995).

According to Krizan and Windschitl (2007), during a risky event, individuals must evaluate the data in light of what they know about that risky event based on their

prior knowledge. The sequence of proceedings while evaluating a situation is as follows: after experiencing a threat, individuals recall related information from memory about that threat; a precise assessment of the danger of the threat is made by utilizing the SEU model; and after assessing the threat, individuals unequivocally pick what conduct to take (Kahneman & Miller, 1986).

3. THEORETICAL FOUNDATION AND HYPOTHESES

The goal of this research is to study the impact of framing and priming on users' behavior in cybersecurity. To generate the hypotheses for this research, prospect theory, instance-based learning theory, and reinforcement theory are used to explain framing and priming in cybersecurity context. The research model is presented in Figure 3.1.

3.1. PROSPECT THEORY

Prospect theory explains one's choices under states of threat (Tversky & Kahneman, 1986). Choices depend on acumen, and acumen relates to evaluation about the exterior conditions of the world. Choices are made specifically tough under states of instability, where it is hard to anticipate the results with certainty or precision. Making choices can be hard when decisions endorse conflicting standards and objectives. The fundamental way to comprehend any rational decision-making condition is to consider the kind of data or information that the user possesses or has access to in order to form the basis of the decision. In the cybersecurity context, both the data and the manner in which the data is framed may influence their judgments and decisions (Tversky & Kahneman, 1984). The process of decision-making by utilizing quantified risks as a metric can be divided into two steps (McDermott, 1991). First, the security risk is assessed by evaluating system susceptibilities and available hazards. Second, the way in which information is presented or framed can influence decision-making (McDermott, 1991).

Prospect theory addresses how decisions are confined and assessed. The key concepts of prospect theory are split into two phases. First, users make decisions by

assessing the risks based on the reference points rather than on final consequences. The impact of this subjective assessment is known as framing, which is the way a prospect is subjectively estimated as either a loss or a gain. This phase involves the organization and reformulation of all the possible options in order to simplify the resulting evaluation and decision (Tversky & Kahneman, 1984). After framing all the possible alternatives, the user assesses each of the alternatives that are perceived as either gains or losses and selects the one with the highest value. Second, judgments are loss-aversive, which means that damages are perceived comparatively stronger than gains (Verendel, 2009).

Framing effect in the prospect theory describes that individuals respond to a specific decision differently by relying upon how it is displayed such as a positive or a negative message (Plous, 1993). Individuals have a tendency to keep away from threats when a positive message is displayed and identify threats when a negative message is displayed (Tversky & Kahneman, 1984). Prospect theory indicates that a damage is perceived to be more substantial than a benefit of the same quantity, i.e., a definite benefit is preferred to a potential benefit and a potential damage is favored over a sure damage (Tversky & Kahneman, 1986). Loss aversion in prospect theory explains that users are more likely to react to losses as compared to gains. Coping evaluation indicates the users' ability to manage and handle any security threat. Efficacy is the users' anticipation that threats can be subdued by following recommendations. Risk appraisal evaluates the vulnerability of the threat and analyzes how critical the threat is (Rogers, 1975). Messages that highlight the adverse consequences of an option are seen as possible damages to which users are likely to react more as compared to the messages

that underlines the profitable results (Tversky & Kahneman, 1984). Based on the prospect theory, we propose that:

H1: Negatively framed security messages will lead users to take a more risk adverse cybersecurity action as compared to positively framed security messages and no security messages.

3.2. INSTANCE-BASED LEARNING THEORY

IBLT (Instance-Based Learning Theory) is a theory of decision making from instance-based knowledge. The IBLT model illustrates how individuals make choices or decisions based on their knowledge of similar instances. IBLT suggests that in dynamic decision-making circumstances, individuals learn by accumulation, identification, and refinement of occurrences. "IBLT proposes that every decision situation is represented as an instance that is stored in the memory. Each instance in the memory is composed of three parts: situation (S) (the knowledge of attributes that describe an event), a Decision (D) (the action taken in a situation) and utility (U) (a measure of the expected result of a decision that is to be made for an event)" (Kanaparthi, Reddy, & Dutt, 2013, p. 331).

According to the IBLT model, two cognitive factors that impact users' discovery of cyber threats are recency and inertia; recency is how user choices rely on similar encounters, and inertia is how users' present verdicts repeat the last made choices. The IBLT's procedure begins with the acknowledgment stage in scanning for choices to characterize a series of incidents as a cyber threat. Amid acknowledgment, an experience or knowledge with the most astounding activation and nearest resemblance with the system incident is recovered from memory and is utilized to make this characterization. Next, in the judgment stage, the recovered knowledge or information is utilized to assess

whether the present incident that is being assessed is seen as a risk or not. A decision is made among the choices based upon inertia or the recency procedure recommended by the model (Gonzalez & Dutt, 2011).

When users are primed with a cybersecurity instance containing information about the outcome of a decision related to that particular situation, the instance gets stored in the users' memory. While experiencing a similar situation, the recognition process takes place and the stored cybersecurity instance gets retrieved from the memory and users make their decision based on the best course of action. Based on the IBLT, we hypothesize that:

H2: Priming users on cybersecurity risks reduces their risk-taking behavior associated with their cybersecurity action.

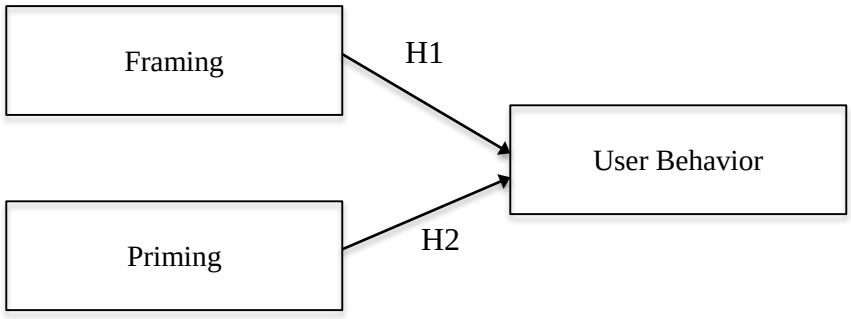


Figure 3.1 Research Model

4. RESEARCH METHODOLOGY

4.1. EXPERIMENTAL DESIGN

We conducted an experimental study and a questionnaire survey study for evaluating the hypotheses, H1 and H2. We recruited undergraduate and graduate subjects from Missouri University of Science & Technology to participate in the experimental and questionnaire survey study. The sample subject size of the experiment was 129. The subjects were provided with a cybersecurity online scenario in order to evaluate their behavior. A between-subject 3 × 2 factorial design was used for evaluating hypotheses H1 and H2. The experimental study had 3 levels for framing (i.e., positive framing, negative framing, and no framing) and 2 levels for priming (i.e., with and without priming). No framing and no priming served as the control conditions.

4.2. RESEARCH PROCEDURES

This research study was conducted in Missouri S & T computer labs. The research procedures are as follows: The cybersecurity scenario involved security threats related to downloading of a media player from a site for online training purposes (Appendix A). The experiment is a 3x2 factorial design with priming and framing as the two independent variables. Appendix B provides the screenshots of all the six experimental conditions. Subjects were randomly assigned to one of the six conditions, and their operationalizations are explained next.

The positively framed security messages emphasizes the advantages of executing security safeguards, for example, dependability, consistency and mental peace for both people and associations. The negatively framed security messages emphasizes the results

of not taking security safety measures, accordingly focusing on the seriousness and likelihood of dangers. Priming was operationalized by providing a user story about a similar security scenario containing the consequences of a known cybersecurity threat.

The subjects were asked to opt for either a safe (not to download) option or a risky (to download) option, which was used to evaluate the users' behavior in dealing with cybersecurity incidents. After completing the cybersecurity online scenario posted to them where subjects made a decision to download or not to download the media player, subjects completed a questionnaire survey based on the 7-point Likert scale (1 = strongly disagree to 7 = strongly agree). In summary, each subject was provided with positively framed security messages or negatively framed security messages or no security message as well as with or without a user story depicting a prior cybersecurity related incident. The scenarios presented to the subjects were completely simulated by a software application, and hence, there was no real risk involved in the study. The survey comprised of questions that helped in measuring perceptual outcomes associated with the users' action (i.e., confidence with action, perceived severity, perceived susceptibility, trust, and fear). We also performed a secondary analysis for assessing the effect of action on perceptual outcomes.

Subjects were provided with a consent form prior to the beginning of the study. The consent form clearly indicated that their participation in the research study is voluntary. It also stated that they might choose not to participate and to withdraw their consent to participate at any time. The consent form indicated that they will not be penalized in any way should they decide not to participate or to withdraw from the study.

Subjects' decisions to download or not to download the media player were captured in order to evaluate the decision or action taken towards the security incident.

4.3. MEASUREMENT

The post-study questionnaire was used to assess the perceptual outcomes associated with user actions, i.e., confidence with action, perceived severity, perceived susceptibility, trust, and fear. It was also used to assess framing and priming manipulation checks, cybersecurity awareness, and background and demographic information of the subjects.

4.3.1. Confidence With Action. The confidence with action scale was used to assess the confidence associated with the subjects' action in downloading the software (see Table 4.1 for the items). The measurement items for confidence with action were developed by the researcher. The 7-point Likert scale (strongly disagree = 1 to strongly agree = 7) was used.

Table 4.1. Measurement Scale for Confidence With Action

	Measurement Items
Confidence With Action	(CONF1) I am confident about the action I took.
	(CONF2) I would choose the same action again.
	(CONF3) I believe I had taken the right action.
	(CONF4) I am confident about my action.

4.3.2. Perceived Severity. The perceived severity scale was used to assess the severity perceived by the subjects in downloading the software (see Table 4.2 for the items). The measurement items for perceived severity were adopted from Johnston and Warkentin (2010). The 7-point Likert scale (strongly disagree = 1 to strongly agree = 7) was used.

Table 4.2. Measurement Scale for Perceived Severity

	Measurement Items
Perceived Severity	(THSV1) If malware would infect my computer, it would be severe.
	(THSV2) If malware would infect my computer, it would be serious.
	(THSV3) If malware would infect my computer, it would be significant.
	(THSV4) Having my identity stolen is a serious problem for me.

4.3.3. Perceived Susceptibility. The perceived susceptibility scale was used to assess the susceptibility of the subjects' action in downloading the software (see Table 4.3 for the items). The measurement items for perceived susceptibility were adopted from Johnston and Warkentin (2010). The 7-point Likert scale (strongly disagree = 1 to strongly agree = 7) was used.

Table 4.3. Measurement Scale for Perceived Susceptibility

	Measurement Items
Perceived Susceptibility	(THSP1) My computer is at risk of becoming infected with malware.
	(THSP2) It is likely that my computer has been infected with malware.
	(THSP3) It is possible that my computer has been infected with malware.

4.3.4. Trust. The measurement items for trust were adopted from Freed (2014) for assessing subjects' trust in the download link (see Table 4.4 for the items). The 7-point Likert scale (strongly disagree = 1 to strongly agree = 7) was used.

Table 4.4. Measurement Scale for Trust

	Measurement Items
Trust	(TRUST1) I believe that the download link is trustworthy.
	(TRUST2) I trust the vendor of the download link.
	(TRUST3) I trust the download link.

4.3.5. Fear. The measurement items for fear were adopted from Freed (2014) for assessing fear in subjects' action in downloading the software (see Table 4.5 for the items). The 7-point Likert scale (strongly disagree = 1 to strongly agree = 7) was used.

Table 4.5. Measurement Scale for Fear

	Measurement Items
Fear	(FEAR1) I was worried about the action I took.
	(FEAR2) I was concerned about the action I took.
	(FEAR3) I experienced fear in the action I took.

4.3.6. Framing Manipulation Check. The manipulation check questions for framing were developed by the researcher (see Table 4.6). These items were included to assess whether the experimental manipulations were effective. Subjects answered on a Yes/No scale.

Table 4.6. Measurement Scale for Framing Manipulation Check

	Measurement Items
Framing	(FRM1) Did the website provide a warning message that informed you about protecting your private information?
	(FRM2) Did the website provide a warning message that informed you about potential exposure of your private information?

4.3.7. Priming Manipulation Check. The manipulation check questions for priming were developed by the researcher (see Table 4.7). These items were included to

assess whether the experimental manipulations were effective. Subjects answered on a Yes/No scale.

Table 4.7. Measurement Scale for Priming Manipulation Check

	Measurement Items
Priming	(PRM1) Did the website provide a User Story that assisted you in guiding your security action?
	(PRM2) Did the website provide a User Story that was relevant to the scenario you faced?

4.3.8. Subject Background Questionnaire. The background questionnaire (see Appendix C) included participant demographics (e.g., gender, age, education, major), Internet usage habits (e.g., Approximately how many hours do you spend online per week?) and cybersecurity awareness questions (see Appendix D).

4.4. PILOT TESTS

We conducted two pilot studies to test the experimental procedures and the experimental conditions. The first pilot study was used to fine-tune and assess the measurement items. The items that did not load well were dropped from the study. The second pilot study was used to fine-tune the experimental procedures and the control conditions. Based on feedback from the pilot studies, modifications were made to the measurement items and the experimental conditions. For example, we added a control condition for framing, thereby modifying the design from 2X2 factorial to 3X2 factorial.

5. DATA ANALYSIS

Subjects were graduate and undergraduate students from Missouri University of Science & Technology. Total number of subjects who participated in the study was 130 out of which 129 subjects successfully completed the experiment because one computer crashed in the middle of the experiment. Hence, the sample size for the study is 129. The sample size consisted of both male and female participants and they were recruited through the help of instructors/professors of classes, forums and email contact.

Demographic details of the subjects are summarized in Table 5.1. The participants were aged between 18 and 44. Factor analysis and validity checks on the measurement scales were conducted. We utilized SPSS 11.0 software to study the data collected.

Table 5.1. Summary of Demographic Details of Subjects

Gender	
Male	65.1%
Female	34.9%
Age	
18-24	93.0%
25-34	6.2%
35-44	0.8%
45-54	0.0%
55-64	0.0%
65-74	0.0%
75 or older	0.0%
Education	
No schooling completed	0.0%
Some high school, no diploma	3.1%
High school graduate, diploma or the equivalent	71.3%
Trade/Technical/Vocational training	3.1%
Associate degree	15.5%
Bachelor's degree	7.0%
Master's degree	0.0%
Professional degree	0.0%
Doctorate degree	0.0%
Online internet usage (per week)	
1-5	3.1%
6-10	12.4%
11-15	26.4%
16-20	20.9%
20+	37.2%
Software downloads	
Once or more per week	13.9%
Two to three times per month	24.8%
Once per month	20.9%
Every few months	22.6%
Rarely or Never	17.8%
Cybersecurity awareness questions	**Yes**
Downloading and installing unlicensed software	50.39%
Use of same password for personal and professional accounts	36.43%
Sharing passwords with others	38.76%
Knowledge of phishing attack	84.50%

5.1. MANIPULATION CHECK ANALYSIS

The findings of the framing manipulation check suggest that there exists a significant difference across the three framing conditions, i.e., no framing, positive framing, and negative framing ($p=0.002<0.05$) for the manipulation check item, FRM1. Manipulation item FRM1 detected positive and negative framing as the p-value of the comparison of positive framing vs. negative framing is 0.0375(1-tailed)<0.05.

The findings of the priming manipulation check suggest that there exists a significant difference between priming and no priming condition ($p=0.001<0.05$) for manipulation item PRM1.

5.2. MEASUREMENT VALIDATION

Statistical tests were conducted at a 0.05 significance level. Exploratory factor analysis (EFA) was carried out to evaluate convergent and discriminant validity for the constructs in the survey questionnaire. EFA results with varimax rotation and principal component analysis are reported in Table 5.2 and Table 5.3. Based on our research model, a five-factor structure was identified with eigenvalues greater than 1.0. All the measurement items loaded onto their target factors respectively and scored above 0.739, which indicates good construct validity (Cook & Campbell, 1979) except for item THSV4. Item THSV4 did not load well; hence we ran the factor analysis again after dropping item THSV4. Table 5.2 reports the factor analysis results with item THSV4 and Table 5.3 reports the factor analysis results without item THSV4.

Table 5.2. Results of Factor Analysis

	Component				
	1	2	3	4	5
CONF4	0.875	-0.067	-0.028	-0.143	-0.142
CONF3	0.846	0.002	-0.004	-0.2	-0.209
CONF2	0.845	0.131	-0.032	-0.141	-0.031
CONF1	0.752	-0.058	0.172	-0.266	-0.01
TRUST2	-0.014	0.93	-0.049	0.06	0.073
TRUST1	0.037	0.925	-0.067	0.051	-0.006
TRUST3	-0.007	0.921	-0.108	0.029	0.042
THSV1	-0.064	-0.052	0.886	0.135	0.037
THSV2	0.029	0.012	0.882	0.074	-0.027
THSV3	0.108	-0.213	0.841	0.128	0.127
FEAR2	-0.199	0.033	0.086	0.847	0.194
FEAR1	-0.298	0.021	0.105	0.82	0.156
FEAR3	-0.23	0.099	0.154	0.772	0.211
THSP3	-0.143	0.063	-0.066	0.222	0.85
THSP1	-0.104	0.027	-0.038	0.228	0.843
THSP1	-0.104	0.027	-0.038	0.228	0.843
THSP2	-0.23	0.094	0.123	0.39	0.739
THSV4	0.042	-0.043	0.336	-0.143	0.489

Table 5.3. Results of Factor Analysis (without item THSV4)

	Component				
	1	2	3	4	5
CONF4	0.873	-0.066	-0.035	-0.16	-0.136
CONF3	0.843	0.132	-0.03	-0.038	-0.148
CONF2	0.84	0.005	-0.003	-0.211	-0.208
CONF1	0.757	-0.059	0.156	-0.066	-0.234
TRUST2	-0.014	0.929	-0.042	0.093	0.048
TRUST1	0.038	0.925	-0.075	-0.009	0.065
TRUST3	-0.007	0.92	-0.105	0.058	0.022
THSV1	-0.063	-0.052	0.898	0.034	0.116
THSV2	0.028	0.013	0.895	-0.027	0.052
THSV3	0.112	-0.214	0.847	0.105	0.122
THSP3	-0.132	0.055	-0.021	0.893	0.153
THSP1	-0.093	0.02	0.003	0.877	0.165
THSP2	-0.221	0.088	0.165	0.787	0.324
FEAR2	-0.197	0.033	0.088	0.228	0.842
FEAR1	-0.295	0.021	0.1	0.179	0.828
FEAR3	-0.225	0.098	0.146	0.221	0.787

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.

The Cronbach's alpha coefficient (Cronbach, 1951) was used to assess the reliability of the measurement. The Cronbach's alpha coefficient for all the five factors is reported in Table 5.4. A value of at least 0.70 indicates adequate reliability (Nunnally, Bernstein, & Berge, 1967). The Cronbach's alpha coefficients for all constructs were well above 0.7, which indicates that all the measurement items achieved high reliability.

Table 5.4. Results of Cronbach's alpha coefficient

Construct	**Cronbach's alpha coefficient**
Confidence with Action	0.88
Perceived Severity	0.87
Perceived Susceptibility	0.88
Trust	0.92
Fear	0.87

5.3. BINARY LOGISTIC REGRESSION ANALYSIS

Binary Logistic Regression is a statistical analysis that is used to predict a categorical or binary outcome i.e., an outcome that has only two possibilities such as Yes/No (Peng, Lee, & Ingersoll, 2002). Binary Logistic Regression is used for dichotomous dependent variables like in this case where the researcher's intention is to know whether the software will be downloaded or not. The results of the binary logistic regression are reported in Table 5.5.

Table 5.5. Results of Binary Logistic Regression

	B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I.for EXP(B)	
							Lower	Upper
Framing			2.363	2	0.307			
Framing(1)	-0.687	0.447	2.362	1	0.124	0.503	0.21	1.208
Framing(2)	-0.344	0.44	0.61	1	0.435	0.709	0.3	1.68
Priming	-0.802	0.363	4.876	1	0.027	0.449	0.22	0.914
Constant	1.488	0.636	5.48	1	0.019	4.429		

In Table 5.5, the statistic given on the Framing row tells us if the dummies that represent Framing, i.e., Framing(1) and Framing(2), taken together, are statistically significant. Column B provides the logit coefficient that indicates the association between the predictor variables (No Framing, Positive Framing, Negative Framing, and Priming) and the dependent variable i.e., Action. Sig column provides the p-value. Coefficients having p-value less than alpha of 0.05 are statistically significant (Peng, Lee, & Ingersoll, 2002).

5.3.1 Framing. We found that Framing ($p = 0.307$) has no significant effect on Action as the p-value is greater than 0.05 (see Table 5.5). Hence, we conclude that framing has no effect on the action taken by the users.

5.3.2. Priming. We found that Priming has a significant effect on Action, i.e., $p = 0.027$ (<0.05) (see Table 5.5). Hence, priming has an effect on the action taken by the users.

5.4. MULTIVARIATE ANALYSIS OF VARIANCE

Multivariate ANOVA (MANOVA) is used when there are two or more continuous dependent variables. MANOVA helps in analyzing whether independent variables have significant effects on dependent variables.

Sig column provides the p-values. Coefficients having p-values less than alpha of 0.05 are statistically significant. Hence coefficients having a p-value of 0.05 or less are statistically significant. Results of MANOVA indicate that Framing and Priming have no significant effect on perceptual outcomes, i.e., Confidence with Action, Perceived Severity, Perceived Susceptibility, Trust, and Fear as their p-values are greater than .05 (see Table 5.6).

We performed the analysis using gender and major as covariates but there was no impact on the MANOVA results. Hence, we haven't included gender and major as covariates in our results as they are not significant.

Table 5.6. Multivariate ANOVA Results

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
Framing	CONFIDENCE WITH ACTION	0.555	2	0.278	0.247	0.781
	PERCEIVED SEVERITY	6.806	2	3.403	2.277	0.107
	PERCEIVED SUSCEPTIBILITY	1.095	2	0.548	0.23	0.795
	TRUST	1.336	2	0.668	0.299	0.742
	FEAR	0.161	2	0.08	0.038	0.963
Priming	CONFIDENCE WITH ACTION	0.668	1	0.668	0.595	0.442
	PERCEIVED SEVERITY	0.527	1	0.527	0.352	0.554
	PERCEIVED SUSCEPTIBILITY	0.053	1	0.053	0.022	0.882
	TRUST	0.869	1	0.869	0.388	0.534
	FEAR	0.087	1	0.087	0.041	0.839
Framing * Priming	CONFIDENCE WITH ACTION	3.776	2	1.888	1.683	0.19
	PERCEIVED SEVERITY	1.969	2	0.984	0.659	0.519
	PERCEIVED SUSCEPTIBILITY	2.669	2	1.335	0.561	0.572
	TRUST	5.908	2	2.954	1.32	0.271
	FEAR	0.784	2	0.392	0.186	0.831

Given that there is no direct effect of framing and priming on the perceptual variables, we will examine the relationship between user behavior and these perceptual variables. The descriptive statistics are shown in Table 5.7 and the results are presented in Table 5.8.

Table 5.7. Descriptive Statistics

	Action	**N**	**Mean**	**Std. Deviation**	**Std. Error Mean**
CONFIDENCE WITH ACTION	Yes	66	5.133	1.093	0.135
	No	63	5.754	0.923	0.116
PERCEIVED SEVERITY	Yes	66	5.05	1.359	0.167
	No	63	5.524	1.031	0.130
PERCEIVED SUSCEPTIBILITY	Yes	66	4.217	1.340	0.165
	No	63	3.567	1.636	0.206
TRUST	Yes	66	4.429	1.275	0.157
	No	63	2.712	1.160	0.146
FEAR	Yes	66	3.470	1.392	0.171
	No	63	3.085	1.446	0.182

Table 5.8. Results of t-test

	t-test for Equality of Means		
	t	**df**	**Sig. (2-tailed)**
CONFIDENCE WITH ACTION	-3.481	127	0.001
PERCEIVED SEVERITY	-2.225	127	0.028
PERCEIVED SUSCEPTIBILITY	2.462	119.935	0.015
TRUST	7.953	127	0
FEAR	1.541	127	0.126

5.4.1. Confidence With Action. We found a significant effect of Action (Action = ‘Yes’ where subjects chose to download the software whereas Action =‘No’ when subjects chose not to download the software) on Confidence with Action, i.e., p = 0.001

(<0.05) (see Table 5.8). Subjects who chose not to download the software, i.e., Action as 'No' (M = 5.754, SD = 0.923) exhibited greater confidence associated with their action than subjects who chose to download the software, i.e., Action as 'Yes' (M = 5.133, SD = 1.093) (see Table 5.7).

5.4.2. Perceived Severity. We found a significant effect of Action (Action = 'Yes' when subjects chose to download the software whereas Action ='No' when subjects chose not to download the software) on Perceived Severity, i.e., p = 0.028 (<0.05) (see Table 5.8). Subjects who chose not to download the software, i.e., Action as 'No' (M = 5.524, SD = 1.031) perceived greater severity associated with cybersecurity risks than subjects who chose to download the software, i.e., Action as 'Yes' (M = 5.05, SD = 1.359) (see Table 5.7).

5.4.3. Perceived Susceptibility. We found a significant effect of Action (Action = 'Yes' when subjects chose to download the software whereas Action ='No' when subjects chose not to download the software) on Perceived Susceptibility, i.e., p = 0.015 (<0.05) (see Table 5.8). Subjects who chose not to download the software, i.e., Action as 'No' (M = 3.567, SD = 1.636) perceived lower susceptibility of their computer to cybersecurity risks than subjects who chose to download the software, i.e., Action as 'Yes' (M = 4.217, SD = 1.340) (see Table 5.7).

5.4.4. Trust. We found a significant effect of Action (Action = 'Yes' when subjects chose to download the software whereas Action ='No' when subjects chose not to download the software) on Trust, i.e., p = 0.00 (<0.05) (see Table 5.8). Subjects who chose not to download the software, i.e., Action as 'No' (M = 2.712, SD = 1.160

perceived lower trust in the download link than subjects who chose to download the software i.e., Action as 'Yes' (M = 4.429, SD = 1.275) (see Table 5.7).

5.4.5. Fear. We found that Action (Action = 'Yes' when subjects chose to download the software whereas Action ='No' when subjects chose not to download the software) has no significant effect on Fear, i.e., p = 0.126 (>0.05) (see Table 5.8).

Table 5.9 shows the results of hypothesis testing. H1 (Negative Framing → Users' Behavior) is not supported, as framing does not have a significant impact on users' behavior. H2 (Priming → Users' Behavior) is supported, suggesting that priming lead users' to take the safer security action.

Table 5.9. Results of Hypothesis Testing

Hypothesis	Supported?
H1: Negatively framed security messages will lead users to take a more risk adverse cybersecurity action as compared to positively framed security messages and no	No
H2: Priming users on cybersecurity risks reduces their risk-taking behavior associated with their cybersecurity action.	Yes

6. DISCUSSIONS

The findings from our study suggest that priming lead users to take a safer security measure, whereas framing has no significant effect on users' behavior in cybersecurity. The findings also suggest that users' action to download or not has a significant effect on confidence with action, perceived severity, perceived susceptibility, and trust whereas users' action has no significant effect on fear.

First, positive and negative framing had no significant impact on users' behavior in cybersecurity ($p > .05$). Thus, our findings posit that, framing does not lead users to take a safe security measure.

Second, priming had a significant impact on users' behavior in cybersecurity ($p < .05$) as compared to no priming (when users were not primed to cybersecurity risks). Our finding is consistent with the instance-based learning theory, which posits that priming is an effective way to reduce cybersecurity risks faced by users.

Lastly, users who had taken a risk adverse cybersecurity action showed greater confidence associated with their action, perceived greater severity associated with cybersecurity risks, perceived lower susceptibility to cybersecurity risks, and perceived lower trust in downloading the software in the experiment.

7. LIMITATIONS AND FUTURE RESEARCH

This study has some limitations, which can be resolved in future research. First, this study was conducted in Missouri S & T computer labs. The reason for doing so was to avoid the hassle for subjects to bring their own laptops. Hence, this study was limited to only lab computers. Future studies can overcome this limitation by asking the subjects to bring their own laptops. This way it can be analyzed whether subjects would respond differently while encountering a security threat on their personal computer versus school computer.

Second, this study did not vary the order of framing and priming, and hence, it could be the recency effect that caused priming to be effective but not framing. Future studies can overcome this limitation by randomizing the order of framing and priming.

Third, many participants felt that the questionnaire was a bit lengthy as there were a lot of demographic questions in the questionnaire. We intended to use the demographic items as covariates in our study so we used a comprehensive subject demographic questionnaire. Future studies can overcome this limitation by further refining the demographic items.

Fourth, we limited our study to analysis of some perceptual outcomes like confidence with action, perceived severity, perceived susceptibility, trust, and fear only. Future studies can be extended to study the effect of action on other perceptual outcomes such as risk and satisfaction.

8. CONCLUSIONS

This research studies the impact of positively and negatively framed security messages and priming on users' behavior in cybersecurity events. This study also analyzes the effect of action on perceptual outcomes of action, i.e., confidence with action, perceived severity, perceived susceptibility, trust, and fear.

Based on the prospect theory, this study focuses on understanding whether negative framing of messages would lead users to take safe security measures as compared to positive framing of messages. The findings suggest that negative framing of messages associated with cybersecurity has no significant effect on users' behavior, or more specifically, their decision to download or not. Based on the instance-based learning theory, this study focuses on understanding whether priming users to cybersecurity risks would lead them to take a safer security action as compared to no priming. The findings suggest that priming has a significant impact on users' behavior, i.e., priming is an effective way to reduce cybersecurity risks faced by users.

Secondary analysis is conducted to study the effect of action on perceptual outcomes. The findings suggest that users who had taken a risk adverse cybersecurity action exhibited greater confidence associated with their action, perceived greater severity associated with cybersecurity risks, perceived lower susceptibility of their computer to cybersecurity risks, and perceived lower trust in the download link they had encountered in the experiment.

The results of this study can benefit in understanding how security messages can enforce users to react to cybersecurity actions and how priming affects users' decision-making while responding to cyber threats.

APPENDIX A.
SCENARIO DETAILS

SCENARIO:
You have just graduated from college and are about to begin your career. It is MANDATORY for you to take a pre-requisite online training before joining a software firm that have offered you a job. The training consists of online videos that are designed to run on the VLC media player. So, you go online and search for the VLC media player, and come across a website that provides the free download facility of the media player.

TASK:
You will be shown the download screen for the VLC Media Player. Complete the rest of the steps after clicking on "Begin" below and complete a questionnaire at the end of the task.

Begin

To view the MANDATORY pre-requisite online training, please click "Download here" to download the media player.

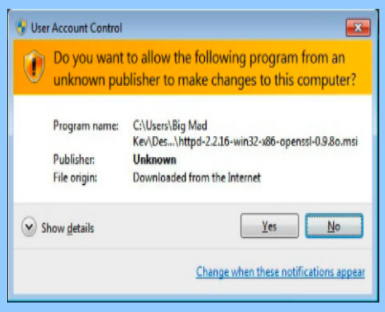
VLC Media Player 2.2.4

Download here

APPENDIX B.

EXPERIMENTAL CONDITIONS FOR 3X2 FACTORIAL DESIGN

1. NEGATIVE FRAMING AND NO PRIMING



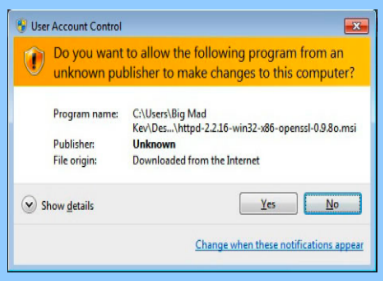
WARNING:

If your choice is "Yes" :
- Your system could be EXPOSED to Malware and Spyware threats
- Your private information could be EXPOSED to the developer of the media player

Do you want to proceed with the download?

Yes No

2. NEGATIVE FRAMING AND PRIMING



WARNING:

If your choice is "Yes" :
- Your system could be EXPOSED to Malware and Spyware threats
- Your private information could be EXPOSED to the developer of the media player

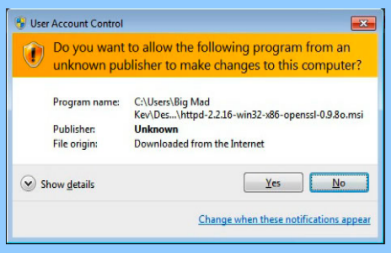
USER STORY:

Recently, a college student tried downloading a media player and received a warning about allowing an unknown publisher to make changes to the computer. He pressed "Yes" and his location details and passwords were collected by the developer of the media player. He got very upset about the invasion.

Do you want to proceed with the download?

○ Yes ○ No

3. POSITIVE FRAMING AND PRIMING



WARNING:

If your choice is "No" :
- Your system will be PROTECTED from Malware and Spyware threats
- Your private information will be PROTECTED from being made available to the developer of the media player

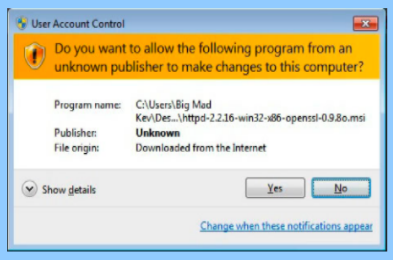
USER STORY:

Recently, a college student tried downloading a media player and received a warning about allowing an unknown publisher to make changes to the computer. He pressed "Yes" and his location details and passwords were collected by the developer of the media player. He got very upset about the invasion.

Do you want to proceed with the download?

○ Yes ○ No

4. POSITIVE FRAMING AND NO PRIMING



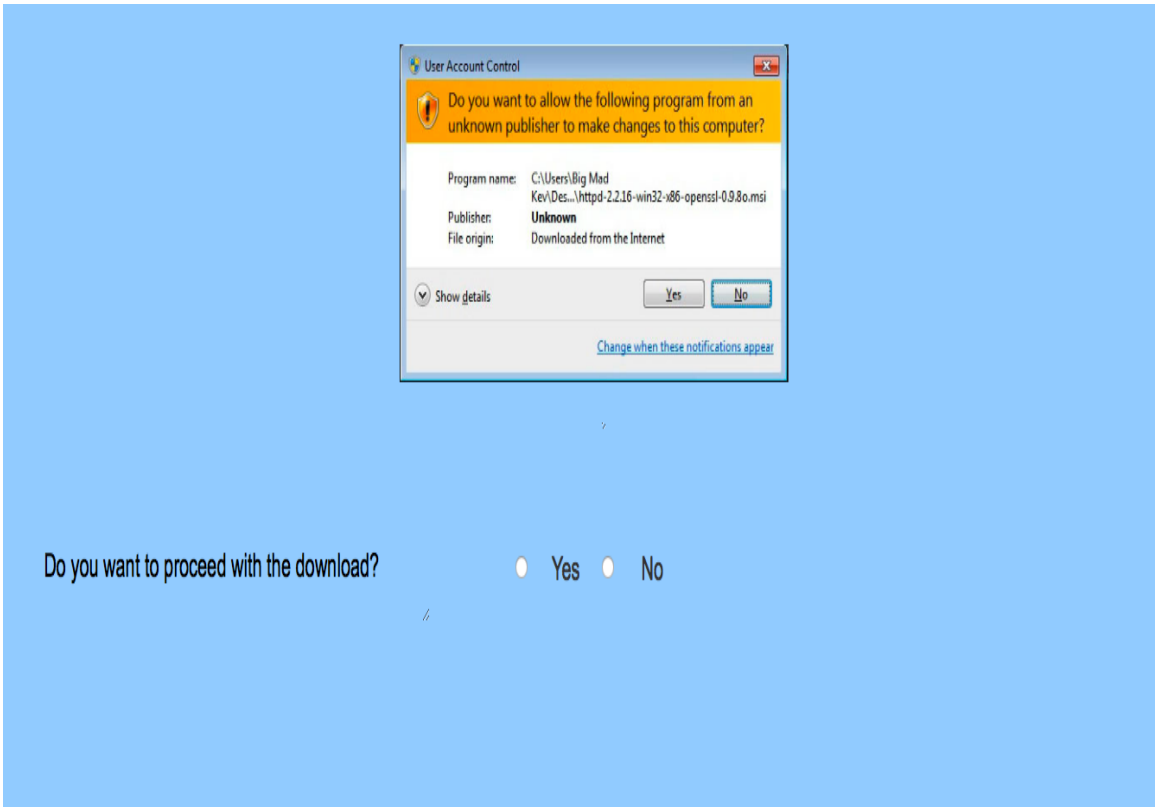
WARNING:

If your choice is "No" :
- Your system will be PROTECTED from Malware and Spyware threats
- Your private information will be PROTECTED from being made available to the developer of the media player

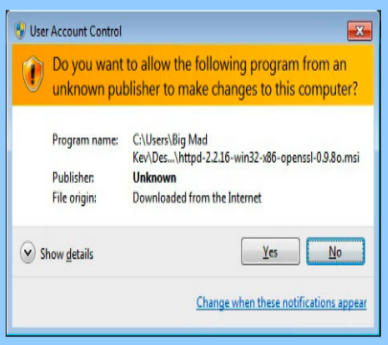
Do you want to proceed with the download?

○ Yes ○ No

5. NO FRAMING AND NO PRIMING



6. NO FRAMING AND PRIMING



USER STORY:

Recently, a college student tried downloading a media player and received a warning about allowing an unknown publisher to make changes to the computer. He pressed "Yes" and his location details and passwords were collected by the developer of the media player. He got very upset about the invasion.

Do you want to proceed with the download?

○ Yes ○ No

APPENDIX C.

SUBJECT BACKGROUND QUESTIONNAIRE

1. Gender - What is your gender? (Male, Female)
2. Age - How old are you? (18-24, 25-34, 35-44, 45-54, 55-64, 65-74 and, 75 or older)
3. What is your major of studies at S&T? (Business Management, Information Science & Technology, Both Business Management and Information Science & Technology, Other)
4. What is your current student status? (Freshman, Sophomore, Junior, Senior, Master's, Other)
5. What is your country of residence? (United States, Other)
6. What is your marital status? (Single, Married, Widowed, Divorced, Separated)
7. What is the highest level of education you have completed, i.e., received (Note: It DOES NOT include the degree you are currently pursuing or that is in progress)? (No schooling completed, Some high school, High school graduate or diploma, Trade/technical/vocational training, Associate degree, Bachelor's degree, Master's degree, Professional degree, Doctorate degree)
8. What is your current employment status? (Employed for wages, Self-employed, Out of work, A homemaker, A student, Military, Retired, Other)
9. What best describes the type of organization you work for? (For profit, Non-profit, Government, Health Care, Education, Other/N.A.)
10. Online - Approximately how many hours do you spend online per week? (1-5, 6-10, 11-15, 16-20, 20+)
11. Approximately how often do you download software from the Internet? (Once or more per month, Two to three times per month, Once per month, Every few months, Rarely or never

APPENDIX D.

CYBERSECURITY AWARENESS QUESTIONNAIRE

1. Do you download and install unlicensed software? (Yes, No)
2. Do you use the same passwords for your school accounts as you do for your personal accounts at home, such as Facebook, Twitter or your personal email accounts? (Yes, No)
3. Have you ever shared your passwords with others? (Yes, No)
4. Do you know what a phishing attack is? (Yes, No)

APPENDIX E.

SUMMARY OF LITERATURE REVIEW

Author (Date)	Description	Theory Applied
(Aaker & Lee, 2001), (Shiv, Edell, & Payne, 2004)	Impact of positively expressed vs. negatively expressed messages on users' decision making.	Prospect Theory
(Tversky & Kahneman, 1986)	Rational choice and Framing: the way a message is outlined impacts the decision making of an individual.	Prospect Theory
(Tversky & Kahneman, 1984)	Author studied that users' are more likely to react to losses than to gains.	Prospect Theory
(Pechmann, Zhao, Goldberg, & Reibling, 2003)	Author used Protection Motivation Theory to classify Efficient Message scenarios.	Protection Motivation Theory
(Siponen, 2000)	Author studied different methods for reducing user related faults and presented critical analysis on strength and weakness of these methods.	Theory of Reasoned Action, Theory of Planned Behavior, Technology Acceptance Model, General Deterrence Theory
(Lebek, Uffen, Breitner, Neumann, & Hohler, 2013)	Four main theories related to human behaviors were discussed.	Protection Motivation Theory, Theory of Planned

		Behavior, Technology Acceptance Model, General Deterrence Theory
(LaRose, Rifon, & Enbody, 2008)	The prospect of refining users' security behavior by highlighting individual's duties in a message. Though, user security behavior depends upon his connection and self-efficacy.	Protection Motivation Theory, Social Cognitive Theory
(Dillon & Tinsley, 2008)	How prior experience or knowledge of risky events influences decision-making under risk.	Not applicable
(Fishbein & Ajzen, 2010)	During risk assessment, individuals utilize the current data, but they also bring prior experiences into their assessment of the hazard.	
(Fox & Tversky, 1995)	SEU model gives a solid foundation for portraying how individuals choose to react to hazards.	Subjective expected utility model

(Dillon, Tinsley, & Cronin, 2011)	According to the disaster literature, user decision-making is influenced by their prior near miss or hit experiences.	Disaster theory
(Johnston & Warkentin, 2010)	Outcomes of this study propose that fear appeals effects users' security behavioral intents but the effect is not constant.	Fear Appeal Theory, Protection Motivation Theory
(Workman, Bommer, & Straub, 2008)	Author studied why end-users who are aware of protecting their network are still unsuccessful in doing so. Outcomes propose that threat appraisal and coping response affect human security behavior.	Protection Motivation Theory, Social Cognitive Theory
(Pahnila, Siponen, & Mahmood, 2007)	Studied that threat evaluation and easing the situations influence attitude.	General Deterrence Theory, Protection Motivation Theory
(Block & Keller, 1995)	Researcher studied the impact of perceived efficacy and message framing on user	Not applicable

	intents.	
(Brewer & Kramer, 1986)	Message framing impacts have been researched from financial and socio psychological standpoints in a diversity of decision-making perspective.	Not applicable
(Lee & Aaker, 2004)	Researcher studied the influence of message framing on risk perceptions	Not applicable
(Lee & Kozar, 2005)	Outcomes of this study propose that attitude and public impact affects users' intents to implement anti-spyware software for network security.	Theory of Planned Behavior
(Stanton, Stam, Mastrangelo, & Jolton, 2005)	Secure password manners are connected to training, mindfulness, monitoring and incentives.	Not Applicable
(Bulgurcu, Cavusoglu, & Benbasat, 2010)	Users' attitude is affected by cost associated with the consequences of his/her compliance/non-compliance behavior.	Theory of Planned Behavior, Rational Choice Theory

BIBLIOGRAPHY

Aaker, J. L., & Lee, A. Y. (2001). "I" Seek Pleasures and 'We' Avoid Pains: The Role of Self-Regulatory Goals in Information Processing and Persuasion,". Journal of Consumer Research , 28 (1), 33-49.

Aytes, K., & Connolly, T. (2004). Computer Security and Risky Computing Practices: A Rational Choice Perspective. Journal of Organizational and End User Computing (JOEUC) , 16 (3), 22-40.

Baker, T. B., Piper, M. E., McCarthy, D. E., Majeskie, M. R., & Fiore, M. C. (2004). Addiction Motivation Reformulated: An Affective Processing Model of Negative Reinforcement. Psychological Review , 111 (1), 33-51.

Block, L. G., & Keller, P. A. (1995). When to Accentuate the Negative: The Effects of Perceived Efficacy and Message Framing on Intentions to Perform Health-Related Behavior. Journal of Marketing Research , 32 (2), 192-204.

Brewer, M. B., & Kramer, R. M. (1986). Choice Behavior in Social Dilemmas: Effects of Social Identity, Group Size, and Decision Framing. Journal of Personality and Social Psychology , 50 (3), 543-549.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quaterly , 34 (3), 523-548.

Cook, T. D., & Campbell, D. T. (1979). Quasi-experimentation : design & analysis issues for field settings (Vol. 351). Boston : Houghton Mifflin.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. Psychometrika , 16 (3), 297–334.

DHS. (2003, February). National Strategy to Secure Cyberspace. Retrieved from U. S. Department of Homeland Security: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

Dillon, R. L., & Tinsley, C. H. (2008). How Near-Misses Influence Decision Making Under Risk: A Missed Opportunity for Learning. Management Science , 54 (8), 1425-1440.

Dillon, R. L., Tinsley, C. H., & Cronin, M. (2011). Why near-miss events can decrease an individual's protective response to hurricanes. Risk Analysis , 31 (3), 440-449.

Fishbein, M., & Ajzen, I. (2010). Predicting and Changing Behavior: The Reasoned Action Approach. New York: Psychology Press.

Fox, C. R., & Tversky, A. (1995). Ambiguity Aversion and Comparative Ignorance. The Quarterly Journal of Economics , 110 (3), 585-603.

Freed, S. E. (2014). Examination of personality characteristics among cybersecurity and information technology professionals. Masters Theses and Doctoral Dissertations.

Gonzalez, C., & Dutt, V. (2011). Instance-based learning: Integrating decisions from experience in sampling and repeated choice paradigms. Psychological Review , 118 (4), 523-551.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006, July). 2006 CSI/FBI Computer Crime and Security Survey. Retrieved Nov 9, 2006, from Computer Security Institute: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.

Hong, J. (2012). The State of Phishing Attacks. Communications of the ACM , 55 (1), 74-81.

IBM Corporation. (2014). IBM Security Services 2014 Cyber Security Intelligence Index. NY.

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quaterly , 34 (3), 549-566.

Kahneman, D., & Miller, D. T. (1986). Norm theory: Comparing reality to its alternatives. Psychological Review , 93 (2), 136-153.

Kanaparthi, B., Reddy, R., & Dutt, V. (2013). Cyber Situation Awareness: Rational Methods versus Instance-Based Learning Theory for Cyber Threat Detection. 12th International Conference on Cognitive Modeling. Ottawa.

Kankanhalli, A., Teo, H.-H., Tan, B. C., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management , 23 (2), 139-154.

Kaplan, S., & Garrick, B. J. (1981). On The Quantitative Definition of Risk. Risk Analysis , 1 (1), 11-27.

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. Communications of the ACM , 51 (3), 71-76.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' Information Security Awareness and Behavior: A Literature Review. 46th Hawaii International Conference on System Sciences (pp. 2978 - 2987). Wailea, HI: IEEE Computer Society.

Lee, A. Y., & Aaker, J. L. (2004). Bringing the Frame into Focus: The Influence of Regulatory Fit on Processing Fluency and Persuasion. Journal of Personality and Social Psychology , 86 (2), 205-218.

Lee, Y., & Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. Communications of the ACM , 48 (8), 72-77.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology , 19 (5), 469-479.

(1991). Prospect Theory. In R. McDermott, Risk-Taking in International Politics (pp. 15-44).

McNeese, M., Cooke, N. J., D'Amico, A., Endsley, M. R., Gonzalez, C., Roth, E., et al. (2012). Perspectives on the Role of Cognition in Cyber Security. Proceedings of the Human Factors and Ergonomics Society Annual Meeting , 56 (1), 268-271.

Nunnally, J. C., Bernstein, I. H., & Berge, J. M. (1967). Psychometric theory (Vol. 226). New York: McGraw-Hill.

Obermiller, C. (1995). The Baby Is Sick/The Baby Is Well: A Test of the Environmental Communication Appeals. Journal of Advertising , 24 (2), 55-71.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. Proceedings of the 40th Annual Hawaii International Conference on System Sciences. IEEE Computer Society.

Pechmann, C., Zhao, G., Goldberg, M., & Reibling, E. (2003). What to Convey in Antismoking Advertisements for Adolescents: The Use of Protection Motivation Theory to Identify Effective Message Themes. Journal of Marketing , 67 (2), 1-18.

Peng, C.-Y. J., Lee, K. L., & Ingersoll, G. M. (2002). An Introduction to Logistic Regression Analysis and Reporting. The journal of educational research , 96 (1), 3-14.

Plous, S. (1993). The psychology of judgment and decision making. McGraw-Hill Education.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. The Journal of Psychology , 91 (1), 93-114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In J. T. Cacioppo, & R. E. Petty, Social Psychophysiology. Guilford , New York.

Shiv, B., Edell, J., & Payne, J. W. (2004). Does Elaboration Increase or Decrease the Effectiveness of Negatively Versus Positively Framed Messages? Journal of Consumer Research , 31 (1), 199-208.

Siponen, M. T. (2000). Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. Information Management & Computer Security , 8 (5), 197-209.

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

Stanton, J., Mastrangelo, P. R., Stam, K. R., & Jolton, J. (2004). Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices. Proceedings of the Tenth Americas Conference on Information Systems. New York.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. Information Systems Research , 1 (3), 255-276.

Thorndike, E. L. (1911). Animal intelligence: Experimental studies. Macmillan.

Tversky, A., & Kahneman, D. (1984). Choice, Values and Frames. American Psychologist , 39 (4), 341-350.

Tversky, A., & Kahneman, D. (1986). Rational Choice and the Framing of Decisions. The Journal of Business , 59 (4), S251-S278.

Wei, L. T., & Yazdanifard, R. (2014). The impact of Positive Reinforcement on Employees' Performance in Organizations. American Journal of Industrial and Business Management , 4 (1), 9-12.

Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: a usability evaluation of PGP 5.0. SSYM'99 Proceedings of the 8th conference on USENIX Security Symposium. 8, pp. 14-14. Berkeley: USENIX Association.

Woon, I., Tan, G.-W., & Low, R. T. (2005). A Protection Motivation Theory Approach to Home Wireless Security. Proceedings of the 26th International Conference on Information Systems, (pp. 367-380). Las Vegas.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior , 24 (6), 2799-2816.

VITA

Kavya Sharma was born in Uttar Pradesh, India. In May 2010, she received her Bachelor's degree in Computer Science from Mody Institute of Technology and Science, India. She worked as a Senior Programmer in Accenture Services Pvt. Ltd, India from June 2010 - Nov 2012. She then joined Missouri University of Science and Technology (formerly University of Missouri – Rolla) in Fall 2015. She earned a Graduate Certificate in Business Analytics & Data Science in Dec 2016 and completed her Master's degree in Information Science and Technology in May 2017. During the course of her Master's degree, she pursued internship with World Wide Technology in 2016.