Spring 2019

Impact of framing and base size of computer security risk information on user behavior

Xinhui Zhan

Department:

IMPACT OF FRAMING AND BASE SIZE OF COMPUTER SECURITY RISK INFORMATION ON USER BEHAVIOR

by

XINHUI ZHAN

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

2019

Approved by:

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

ABSTRACT

This research examines the impact of framing and base size of computer security risk information on users' risk perceptions and behavior (i.e., download intention and download decision). It also examines individual differences (i.e., demographic factors, computer security awareness, Internet structural assurance, self-efficacy, and general risk-taking tendencies) associated with users' computer security risk perceptions. This research draws on Prospect Theory, which is a theory in behavioral economics that addresses risky decision-making, to generate hypotheses related to users' decision-making in the computer security context. A 2 × 3 mixed factorial experimental design (N = 178) was conducted to assess the effect of framing and base size on users' download intentions and decisions. The results show that framing and base size of computer security risk information are associated with users' perceived risk and risk-taking behavior. More specifically, negative framing and large base size increase users' perceived risk and reduce users' risk-taking behavior. Moreover, users who have greater general risk-taking tendencies and perceive higher Internet structural assurance exhibited lower risk perceptions and greater risk-taking behavior in the computer security context. The findings from this research suggest that using negative framing and large base size to communicate computer security risk information is an effective way to lower risk-taking behavior of users.

Keywords: Framing, Computer Security, Risk, Decision-making

ACKNOWLEDGMENTS

I am extremely fortunate to have my committee members: Dr. Fiona Fui-Hoon Nah, Dr. Keng Siau and Dr. Richard Hall. I have learned so much from these amazing scholars and their guidance in my path to becoming a researcher. I am grateful to them for their crucial remarks that shaped this thesis. I would like to express my gratitude to my advisor, Dr. Fiona Nah. This thesis would have been impossible without her support, guidance, and encouragement. Her patience, knowledge, and vast experience in research have been exceptional. It has been a great learning experience under her guidance.

I am also grateful to have the learning environment offered by the Department of Business and Information Technology and the professors who opened an academic window for me. The opportunities created by the faculty, and supported by administrators and staff, make learning a joyous and meaningful experience.

I would like to thank the Center for Technology Enhanced Learning (CTEL) for the financial support in recruiting subjects. I would like to express my gratitude to all the Laboratory of Information Technology and Evaluation (LITE) students for pilot testing the experimental study. I also thank National Science Foundation for the research funding.

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

Finally. I am truly grateful to my parents, who provided me with endless love and faith.

TABLE OF CONTENTS

Page

ABSTRACT iii

ACKNOWLEDGMENTS iv

LIST OF ILLUSTRATIONS viii

LIST OF TABLES ix

SECTION

1. INTRODUCTION 1
2. LITERATURE REVIEW 3
   - 2.1. COMPUTER SECURITY DECISION-MAKING 3
   - 2.2. SUSCEPTIBILITY TO COMPUTER SECURITY THREATS 4
   - 2.3. FRAMING EFFECTS IN CYBERSECURITY DECISION-MAKING 7
3. THEORETICAL FOUNDATION AND HYPOTHESES 11
   - 3.1. THEORETICAL FOUNDATION 11
     - 3.1.1. Prospect Theory 11
     - 3.1.2. Theory of Reasoned Action and Theory of Planned Behavior 14
     - 3.1.3. Technology Acceptance Model 17
   - 3.2. HYPOTHESES AND RESEARCH MODEL 18
4. RESEARCH METHODOLOGY 23
   - 4.1. SUBJECTS 23
   - 4.2. RESEARCH PROCEDURES 23
   - 4.3. VARIABLES AND OPERATIONALIZATION 24
     - 4.3.1. Framing 25

4.3.2. Base Size 25
4.4. MEASUREMENT 27
4.4.1. Perceived Risk 27
4.4.2. Download Intention 28
4.4.3. Download Decision 28
4.4.4. General Information Security Awareness 28
4.4.5. Self-Efficacy 29
4.4.6. Cybersecurity Awareness 30
4.4.7. Internet Structural Assurance 30
4.4.8. General Risk-Taking Tendencies 30
4.4.9. Computer Security Risk-Taking Tendencies 31
4.4.10. Framing Manipulation Check 32
4.4.11. Subject Background Questionnaire 32
5. DATA ANALYSIS 33
5.1. DEMOGRAPHIC INFORMATION OF SUBJECTS 33
5.2. MEASUREMENT VALIDATION 36
5.3. REPEATED MEASURES ANALYSIS OF VARIANCE 40
5.3.1. Check for Assumptions 41
5.3.2. Results of Repeated Measures ANOVA 43
5.3.2.1. Tests of between-subjects effects (framing) 43
5.3.2.2. Tests of within-subjects effects (base size) 47
5.4. MIXED MODEL REGRESSION ANALYSIS 50
6. DISCUSSIONS 53
7. LIMITATIONS AND FUTURE RESEARCH 55

8. CONCLUSIONS 57

APPENDICES

A. SCENARIO DETAILS 60

B. EXPERIMENTAL CONDITIONS 62

C. QUESTIONNAIRE 66

D. QUESTIONNAIRE OF DEMOGRAPHICS INFORMATION 69

BIBLIOGRAPHY 72

VITA 77

LIST OF ILLUSTRATIONS

Page

Figure 3.1. Value Function 14

Figure 3.2. Theory of Planned Behavior and Theory of Reasoned Action..... 17

Figure 3.3. Technology Acceptance Model..... 18

Figure 3.4. Research Model..... 22

Figure 5.1. SPSS Explore Output: Boxplot for Perceived Risk in Small Base Size..... 42

Figure 5.2. SPSS Explore Output: Boxplot for Perceived Risk in Medium Base Size 42

Figure 5.3. SPSS Explore Output: Boxplot for Perceived Risk in Large Base Size..... 42

Figure 5.4. Main Effect of Framing Across Three Levels of Base Size..... 44

LIST OF TABLES

Page

Table 2.1. Summary of Research on Susceptibility to Computer Security Threats 7

Table 2.2. Summary of Research on Framing Effects on Decision-Making 10

Table 4.1. Operationalization of Base Size in Positive Framing 26

Table 4.2. Operationalization of Base Size in Negative Framing..... 26

Table 4.3. Measurement Scale for Perceived Risk 27

Table 4.4. Measurement Scale for Download Intention 28

Table 4.5. Measurement Scale for General Information Security Awareness..... 29

Table 4.6. Measurement Scale for Self-Efficacy 29

Table 4.7. Measurement Scale for Cybersecurity Awareness 30

Table 4.8. Measurement Scale for Internet Structural Assurance 31

Table 4.9. Measurement Scale for General Risk-Taking Tendencies 31

Table 4.10. Measurement Scale for Computer Security Risk-Taking Tendencies..... 32

Table 5.1. Summary of Demographic Details of Subjects..... 33

Table 5.2. Results of Exploratory Factor Analysis (with all measurements) 36

Table 5.3. Results of Factor Analysis (after removing GISA, CSRT, and CA6) 38

Table 5.4. Results of Reliability Analysis 40

Table 5.5. Descriptive Statistics of Between-Subjects Effects for Framing..... 44

Table 5.6. Tests of Between-Subjects Effects 46

Table 5.7. Descriptive Statistics for Perceived Risk at Three Levels of Base Size..... 47

Table 5.8. Tests of Within-Subjects Effects of Base Size 48

Table 5.9. Results of the Bonferroni Post-Hoc Tests..... 49

Table 5.10. Tests of Perceived Risk Effects on Download Decision 50

Table 5.11. Tests of Download Intention Effects on Download Behavior 51

Table 5.12. Results of Hypothesis Testing 52

1. INTRODUCTION

Computer security threats are common on the Internet. To reduce cybersecurity risks and protect users' private information, computer security scientists are working toward providing security warnings, security indicators, pop-up windows, and other types of warning systems when users are at risk of cybersecurity threats. Users play a fundamental role in identification and prevention of computer threats (Stanton et al., 2004). They are expected to assess cybersecurity threats before they conduct online transactions, access a URL, or download files or applications. For example, users make decisions related to downloading software from anonymous sources and providing personal information to conduct online transactions. Their choices could bring negative outcomes, such as data and information leakage and damage to their personal computer.

A report by IBM indicates that more than 95% of the security occurrences in IBM were attributed to human errors (IBM Corporation, 2014). As the "weakest link" in the security chain, people sometimes fail to detect threats. Users' ability to identify security risks is crucial in an online environment. Therefore, it is important to study users' behavior in the computer security context.

Identification of security risks is dependent on users' perceptions and behavior toward potential threats. Some of the previous studies on cyber threats have focused on comparing physical or structural cues and miscues (Jakobsson & Ratkiewicz, 2006; Darwish & Bataineh, 2012; Smith et al., 2016). They also looked at Internet users' ability to interpret cues and miscues that are embedded in web pages or emails. Moreover, researchers have studied human factors that are associated with users' online behavior, including individual differences, gender differences, human cognitive limitations, and

other factors influencing how users distinguish between legitimate and fraudulent messages (Dhamija et al., 2006; Downs et al., 2006).

Aytes and Conolly's (2004) decision model suggests that users' online behavior is driven by their assessment of the outcomes of risk-averse and risk-taking actions. Their study shows the importance of cybersecurity knowledge and awareness, as well as the impact of hazard attitudes on behavior. A crucial aspect of users' behavior in cybersecurity is how users assess and perceive the messages of computer threat warnings. Thus, users' risk perceptions play a crucial role in attaining computer security.

The goal of this research is to explore how computer security risk information can be presented to reduce users' risk-taking decision-making and behavior. A laboratory experiment was conducted to examine the impact of framing of cyber security scenarios and presentation of risk information of different base sizes on users' risk perceptions and behavior. Specifically, we are interested in studying whether negatively framed messages give rise to risk-averse actions more than positively framed messages and whether increasing the base size of the evidence of computer threats decreases users' risk-taking behavior.

This thesis is organized as follows. Section 2 presents a review of related literature. Section 3 presents the theoretical foundation and hypotheses. Section 4 describes the research methodology, design, and procedure. Section 5 and Section 6 present and discuss the findings. The limitations and future research directions are presented in Section 7. Section 8 concludes the thesis.

2. LITERATURE REVIEW

Research on usable computer security has focused on understanding human factors and improving systems to foster safer user behavior in the context of computer security. This section provides a review of the literature on human factors in computer security, especially in the context of users' susceptibility to cyber-attacks.

2.1. COMPUTER SECURITY DECISION-MAKING

Understanding the human cognition and decision-making process is key to explain users' behavior when faced with cybersecurity threats. Hence, we need to open up the 'black box' in order to understand users' cyber decisions, such as decisions to click through a link embedded in an email, download files from websites, or enter personal information on e-commerce websites or social media.

Several studies have focused on developing better interface and warning design to get the attention of users in order to foster safer cybersecurity behavior. Researchers have studied security warnings from multiple perspectives. In a laboratory study to assess the effectiveness of phishing warnings, it was found that more than 90% of the participants fell into the trap of phishing emails without any warnings (Egelman et al., 2008). On the contrary, when active warnings were popped up on the screen, 79% of the participants avoided the phishing attack. Based on these findings, it was recommended that warnings or indicators be provided to convey recommended actions to users even though they may interrupt the users' work. In a large-scale field study that assessed the effectiveness of browser security warnings on the Firefox and Chrome's telemetry platform, it was found that more participants entered personal information when there were no active warning

indicators than when active warning indicators were provided (Akhawe & Felt, 2013). The findings in another study indicate that opinionated framing or design increases adherence by users through decreasing the rate of click-through of SSL warnings (Felt et al., 2015).

Smith, Nah, and Cheng (2016) examined user assessment of security levels in e-commerce by varying cues/miscues (i.e., HTTP vs. HTTPS, fraudulent vs. authentic URL, padlocks beside fields) presented on web pages. They conducted a within-subjects experiment where users rated their perceived security, trustworthiness, and safety after examining each of the e-commerce web pages that vary in these cues/miscues. They found that padlocks provided beside a field (i.e., miscues) do not affect user perceptions of security but primed subjects to look for more important security cues, such as HTTP vs. HTTPS.

2.2. SUSCEPTIBILITY TO COMPUTER SECURITY THREATS

Human factors, such as past experience, culture, and concerns with Internet security, are expected to influence user security behaviors. In a study that investigated the relationship between demographic characteristics and phishing susceptibility, participants were asked to complete a background survey before they proceeded to a roleplay on phishing, where they were asked to click on a phishing link or enter personal information on phishing websites (Sheng et al., 2010). The study discovered two predictors of phishing susceptibility: gender and age. Specifically, the results indicated that women were more likely than men to fall into the phishing trap. The authors provided a possible reason for the gender difference by suggesting that women tend to have less technical knowledge than men. Moreover, individuals of 18-25 years of age were more susceptible

to phishing. This group appears to be more susceptible because participants in this age group have lower levels of education, less experience on the Internet, and less of an aversion to risks.

Flores, Holm, Nohlberg, and Ekstedt (2015) examined the influence of demographic, cultural, and personal factors on phishing. Participants from nine organizations in Sweden, USA, and India participated in their survey to compare users' behavior in response to phishing attacks across users of different cultural backgrounds. The results did not indicate any relationship between phishing and age or gender, but they found that intention to resist social engineering, formal IS training, computer experience, and computer security awareness have a significant effect on reactions to phishing. Additionally, the results indicate that the correlation between phishing determinants and employees' actual phishing behavior differs between Swedish, US, and Indian employees.

In a study by Goel, Williams, and Dincelli (2017), phishing emails were sent to more than 7000 undergraduate students and their responses to the phishing emails were recorded. The phishing message contained different rewards, such as a gift card, tuition assist, and a bank card. The results show that susceptibility varies across users with different demographics (i.e., major and gender). Females were more likely to open phishing emails, with an overall rate of 29.9% compared to 24.4% among males, and the rate varies based on the content in the emails. Participants with business education background had the highest opening/clicking link rate compared to those with social science, business and STEM background. Based on the results, the authors suggest developing context-based education to decrease susceptibility to phishing attacks on the Internet.

In another study that examined the effect of gender and personality on phishing, females were found to be more vulnerable to phishing (Halevi et al., 2013). In their study, 53% of women were phished as compared to 14% of men. The authors attributed the behavior to females being more comfortable with online shopping and digital communication than males. Moreover, they found that people who fell into the phishing trap have very high neuroticism. A possible explanation that neuroticism could result in susceptibility to phishing attacks is that neuroticism may cause people to be more upset when being deceived and therefore, people rather believe that things and people are generally truthful.

Vishwanath (2015) studied the influence of e-mail habits and cognitive processing on phishing susceptibility. Phishing emails were sent to college students to assess their responses. The students were asked to complete a survey on their background and demographic information. The results indicate that e-mail habits are determined by individual personality traits of conscientiousness and emotional stability, and cognitive processing was premised on information adequacy. Basically, there are two routes of cognitive processing: heuristically and systematically (Chaiken & Eagly, 1989). Heuristic processing uses judgmental rules that are learned and stored in memory, whereas systematic processing includes comprehensive and analytic processing of judgement-relevant information. This study found that heuristic processing and strength of email habits led to an increase in victimization.

Table 2.1 provides a summary of the influence of user characteristics on susceptibility to computer security threats.

Table 2.1. Summary of Research on Susceptibility to Computer Security Threats

Reference	Research Focus	Summary of Findings
Sheng et al., 2010	Investigated the relationship between demographic characteristics and phishing susceptibility	Females are more susceptible to phishing email than males.18-25-year-old individuals formed the most susceptible age group.
Flores et al., 2015	Examined the influence of demographic, cultural, and personal factors on phishing	The results did not find any relationship between phishing and age or gender, but they found that intention to resist social engineering, formal IS training, computer experience, and computer security awareness have a significant effect on reactions to phishing.
Goel et al., 2017	Explored if susceptibility varies across users with different demographics (i.e., major and gender)	Females were more likely to open phishing emails, with an overall rate of 29.9% comparing to 24.4% among males, but the rate varies based on the content in the emails. Participants with business education background had the highest opening/clicking link rate compared to those with social science, business and STEM background.
Halevi et al., 2013	Examined the effect of gender and personality on phishing	Females were found to be more vulnerable to phishing. Neuroticism is correlated with susceptibility to phishing.
Vishwanath, 2015	Studied the influence of e-mail habits and cognitive processing on phishing susceptibility	Heuristic processing and email habits led to an increase in victimization.

2.3. FRAMING EFFECTS IN CYBERSECURITY DECISION-MAKING

Prospect theory suggests that decision-making under risk depends on whether the potential outcome is perceived as a gain or a loss (Kahneman & Tversky, 1979). Tversky and Kahneman (1981) proposed that choices between options can be affected by the

framing of the options. Their findings indicate that people tend to avoid risks under gain frames but seek risks under loss frames. Moreover, losses have a greater impact on people's decision-making than gains. In addition, when subjects were required to explain their choices, the framing effect tended to be reduced (Larrick et al., 1992). The framing effect could be eliminated if users are encouraged to think through the rationale underlying their choices (Takemura, 1994). Also, if users are experts in a particular area, the framing effect will also be reduced (Davis and Bobko, 1986).

Various researchers have utilized prospect theory to study users' behavior in the information science field. They evaluate the impact of positively vs. negatively framed messages on users' decision-making, including financial decisions (Brewer & Kramer, 1986), idealness of messages, perceived prominence (Aaker & Lee, 2001), and threat awareness (Lee & Aaker, 2004).

However, the results of empirical studies on the effect of framing are not consistent. An experiment conducted by Rosoff, Cui, and John (2013) examined the effect of gain and loss framing on user decisions, including downloading a music file, installing a plug-in for an online game, and downloading a media player to legally stream video. The study investigated whether and how human decision-making depends on gain-loss framing and the salience of a prior near-miss experience. They examined one kind of near-miss experience, resilient near-miss, which refers to the case where a user had a near-miss experience on a cyber-attack. They carried out a 2 x 2 factorial design and manipulated two levels of each of the two independent variables: frame (gain vs. loss framing) and previous near-miss experience (absence vs. presence). Their results indicate that users tend to follow a safe practice when they have prior experience with a near-miss cyber-attack. They also concluded that females are more likely to select a risky choice

compared to males. Unexpectedly, the results suggest that subjects were indifferent between safe versus risky decision options when the outcomes were framed as gains or losses.

Cybersecurity researchers also expand the definition of "gain-loss" framing. In Valecha et al.'s (2016) study, "gain" was operationalized using a reward-based phishing email and "loss" was operationalized using a risk-based phishing email. Reward-based persuasion is designed to attract users by offering a reward or benefit. For example, emails that inform the recipient about winning a lottery. On the other hand, risk-based persuasion is designed to scare people by highlighting a potential risk. The study found that the presence of both reward-based persuasion (gain frame) and risk-based persuasion (loss frame) increase response likelihood.

Chen, Gates, Li, and Proctor (2015) conducted three experiments to assess the influence of negatively and positively framed summary of risk information on app-installation decisions. Risk information was framed as the amount of risk (negative framing) or amount of safety (positive framing) in the experimental conditions. The results suggest that the summary that was positively framed (as the amount of safety) has a greater effect on app-installation decisions than the negatively framed (as the amount of risk) summary. Hence, a valid index that is framed positively by focusing on safety can be developed to increase users' app-installation decisions.

Table 2.2 provides a summary of the literature on the effects of framing on decision-making.

Table 2.2. Summary of Research on Framing Effects on Decision-Making

Reference	Research Focus	Summary of Findings
Tversky & Kahneman, 1981	Impact of monetary losses and gains on users' behavior	Users perceived losses more seriously than gains.
Beebe et al., 2014	Effect of framing of messages on user's financial decision	Users tend to be more risk-taking when presented with a case of financial losses than gains.
Chen et al., 2015	The influence of summary risk information on app-installation decisions	Positive framing (safety index) decreases users' risk-taking behavior
Rosoff et al., 2013	The influence of gain-loss framing on decision-making	Subjects were indifferent between safe versus risky decision options when the outcomes were framed as gains or losses.
Valecha et al., 2016	The effect of reward-based vs. risk-based phishing email on response	Both reward-based and risk-based phishing email in phishing increases response likelihood.

3. THEORETICAL FOUNDATION AND HYPOTHESES

Section 3 review theories from behavioral science and psychology to provide the foundation for this research.

3.1. THEORETICAL FOUNDATION

We draw on theories from behavioral science and psychology to provide the foundation for this research. Specifically, we draw on the principles of decision making under risks and uncertainty in Prospect Theory to analyze user perceptions associated with computer security, and Theory of Reasoned Action, Theory of Planned Behavior, and Technology Acceptance Model to generate hypotheses on user behavior in the context of computer security.

3.1.1. Prospect Theory. People do not always make rational decisions because they value gains and losses differently. Prospect theory is a descriptive theory that focuses on this phenomenon and addresses how people make decisions when they are facing choices involving risks and uncertainty (e.g., different likelihood of gains and losses). Tversky and Kahneman (1981) proposed that people make choices based on the phrasing or framing of the options. They also explored how different framing affects choices in a hypothetical life and death situation in 1981, which is known as the "Asian disease problem". The subjects were told that "the U.S. is preparing for the outbreak of an unusual Asian disease, which is expected to kill 600 people" (Tversky and Kahneman, 1981, p. 453). They were provided with two options, one predicted to result in 400 deaths, whereas the other one predicted 33% chance that everyone would live and 67% chance that everyone would die.

Half of the subjects were given two positively framed options:

A. 200 people will be saved (a certain outcome)

B. 1/3 probability of saving 600 people and 2/3 probability of saving none (an uncertain outcome)

The other half of the subjects were given two negatively framed options:

C. 400 people will die (a certain outcome)

D. 1/3 probability that none will die and 2/3 probability that 600 will die (an uncertain outcome)

Expected Utility Theory (Mongin, 1997), which is an alternate theory to prospect theory in decision-making, assumes that the choice people made is of the highest satisfaction to the decision maker. From the perspective of Expected Utility Theory, the two options (i.e., a certain one and an uncertain one) in positive framing are mathematically equivalent to the two options in negative framing since they provide the same utility (satisfaction). “200 people will be saved” implies that among 600 people, there are 200 people will surely be saved, so one-third of the 600 people will not die. While “400 people will die” in the negative frame implies that two-thirds of the 600 people will die. As a result, subjects are expected to choose the option in a similar way regardless of the frame of the problem. In other words, based on Expected Utility Theory, the percentage of risky choices is expected to be the same (or at least similar) in both framing.

Surprisingly, in the positively framed scenario, 72% of the subjects selected the certain option and 28% selected the risky option. On the contrary, in the negatively framed scenario, only 22% of the subjects selected the certain outcome and 78% selected the risky option. The results suggest that when provided with positive prospects, people

are more willing to go for the certainty of saving 200 people and refuse the possibility that no one will be saved. On the other hand, when provided with negative prospects, people would rather pursue the option with uncertainty, due to the fear of a large loss of 400 people's lives. In other words, people have the tendency to avoid losses and optimize for sure wins since the pain of losing is greater than the satisfaction of an equivalent gain. Thus, people are risk-averse in positive framing and risk seeking in negative framing. This phenomenon that is termed "Framing Effect" describes a common cognitive bias in decision-making.

Prospect theory uses two factors to explain the framing effect: the reference point, and the value function. The reference point refers to the status quo, determining how the outcomes are framed, either positively or negatively. When outcomes are greater than the reference point, they will be considered as gains, while they will be considered as losses when the outcomes are less than the reference point. Kahneman and Tversky (1979) used a value function to explain and depict the difference in risk preferences among choices involving gains and losses. The value function is a cubic parabola type curve, which is nearly asymmetrical in gain and loss domains (see Figure 3.1). The gain side is concave which suggests that people are risk-averse when people make choices involving gains, whereas the loss side of the curve is convex, indicating that people tend to be risk-seeking when they make choices involving losses. Moreover, the value function is steeper for losses than gains, representing individuals weighing losses more heavily than gains.

In the "Asian disease" problem, the reference points in each framing are different. The positive framing refers to saving lives, so the status quo is "zero people saved", thus both options suggest a potential gain. In the opposite, the negatively framed problem refers to death. The reference point, in this case, is "zero people died" so the two options

can be viewed as losses. Drawing on the value function, the result of the Asian Disease problem can be explained as follows: the risky option is preferred in negative framing because people are risk-seeking in order to avoid larger losses; the option with certainty is preferred in positive framing because people are risk-averse and more willing to go with sure gains.

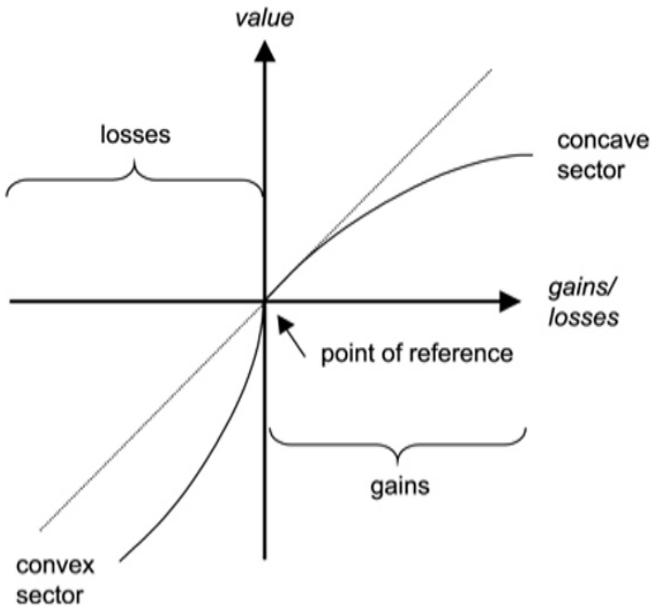

Figure 3.1. Value Function

3.1.2. Theory of Reasoned Action and Theory of Planned Behavior. Theory of Reasoned Action (TRA) and Theory of Planned Behavior (TPB) provide a theoretical foundation for modelling users' behavior in the computer security context.

TRA is a psychology theory that links people's attitude and behavior (Fishbein & Ajzen, 1967). It examines the relationship among attitude, subjective norm, behavioral intention, and behavior. This theory states that individual's behavior is based on their pre-existing attitudes and behavioral intentions. Basically, one's decision to engage in a particular behavior is based on motivation to perform the behavior, which can be considered as the individual's expectation of the outcome of performing a particular action. To be more specific, people's behavioral intention to perform a behavior is the main predictor of their actual behavior. Behavioral intention is the intention to perform the behavior, which precedes the actual behavior and is determined by attitudes and subjective norms.

TPB focuses on explaining the relationships between attitude, subjective norm, perceptional behavioral control, behavioral intention, and behavior (Ajzen, 1991). It proposes that one's behavioral intention is shaped by attitude toward behavior, subjective norms, and perceived behavioral control, while behavioral intention is the key predictor of behavior. As an extension of TRA, TPA includes behavioral control as an additional determinant of intention and behavior. In sum, to predict whether an individual intends to perform a behavior, we need to know whether the person is in favor of performing the action (i.e., attitude), how much social pressure the person feels about performing the action (i.e., subjective norm), and whether the person feels in control of performing the action (i.e., perceived behavioral control).

TRA and TPB are often applied in behavioral research. Figure 3.2 shows the combined model of TRA and TPB, which includes the following key concepts:

- Behavioral Beliefs. This concept explores people's motivations of a particular behavior in terms of the behavior's outcome. In fact, people tend to associate

the performance of a particular behavior with a set of outcomes or features. For instance, if a person believes that preparation for a test leads to success, the behavioral belief is that preparation is associated with success whereas no preparation is associated with failure.

- Evaluations of the Behavioral Outcome. This concept refers to how people perceive and evaluate the potential outcomes of performing a behavior.
- Attitudes. It is one of the key determinants of behavioral intention and addresses the way people feel about a particular behavior. Attitudes are influenced by behavioral beliefs and evaluation of the behavioral outcome.
- Normative Beliefs. It refers to a person's perception of social normative pressures or other relevant beliefs that determine whether or not he or she should perform the behavior.
- Motivation to Comply. This concept focuses on whether a person will comply with social normative pressures.
- Subjective Norms. Ajzen (1991) defines this term as "perceived social pressure to perform or not perform the behavior". It is one of the key determinants of behavioral intention. It refers to the fact that one's perception of the particular behavior is influenced by his or her surrounding, such as family members and friends.
- Control Beliefs. It refers to an individual's beliefs about the presence of factors that may assist or impede the performance of the particular behavior.
- Perceived Power. This concept refers to the perceived presence of factors that may assist or impede the performance of the particular behavior.

- Perceived Control. It is one of the key determinants of behavioral intention. It is defined as a person's perceived ease or difficulty of performing the particular behavior.
- Intention. This refers to the motivational factors that influence a given behavior where the stronger the intention to perform the behavior, the more likely the behavior will be performed.

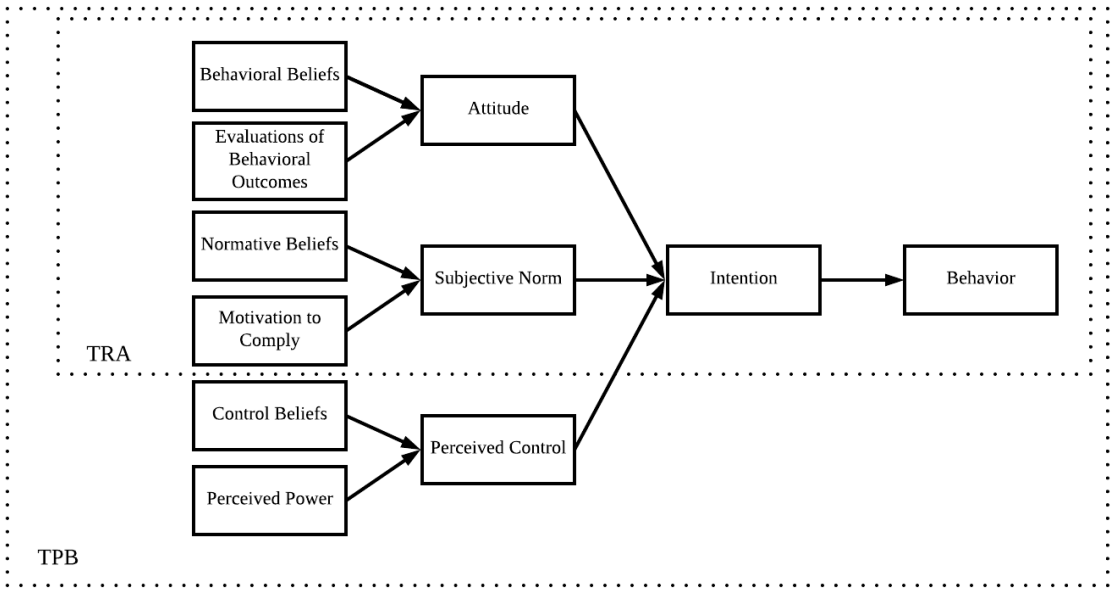

Figure 3.2. Theory of Planned Behavior and Theory of Reasoned Action

3.1.3. Technology Acceptance Model. Technology Acceptance Model (TAM) is an adaptation of TRA/TPB and it is an information system theory that models users' acceptance of information technology (Davis et al., 1989). TAM replaces some of TRA/TPB's measures of attitude with two technology acceptance measures, perceived

ease of use and perceived usefulness. The model proposes that users' acceptance of a system is directly determined by behavioral intention to use the system, which is in turn determined by the users' attitudes toward the technology and the perceived usefulness of the technology. Moreover, attitude and perceived usefulness are influenced by perceived ease of use (see Figure 3.3). Perceived usefulness reflects an individual's belief in the system, and it is positively related to attitude toward using the system and behavioral intention to use the system. Perceived ease of use is defined as a person's belief that using the technology will be free of effort (Davis et al., 1989).

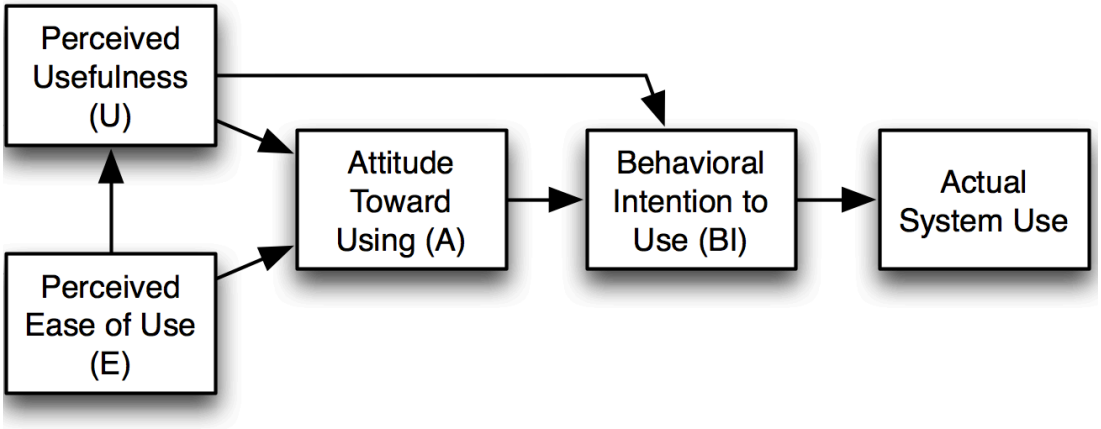

Figure 3.3. Technology Acceptance Model

3.2. HYPOTHESES AND RESEARCH MODEL

Prospect theory purports that individuals weigh losses more heavily than gains. Hence, the framing of outcomes affects users' perceptions because losses exert a stronger influence over people's perceptions than gains. We extend the term "gains and losses" to

two different and opposite ways to present information. When a situation is framed negatively, the negative consequences or attributes are emphasized. When a situation is positively framed, the positive aspects are more salient. For example, the Asian Disease problem can be presented as "400 of 600 people will be saved" or "200 of 600 people will die"; similarly, a piece of meat can be presented as "75% fat-free" or "25% fat".

Based on prospect theory, we hypothesize that the framing of the possible consequences of a risky action affects users' perceived risk. Specifically, negative framing leads to greater perceived risk than positive framing because losses exert a stronger influence over people's perceptions than gains. Positive framing is in the domain of gains as it highlights the assurance of keeping the computer system secure whereas negative framing is in the domain of losses as it accentuates the hazard to computer security. Such an explanation is consistent with prospect theory and it extends prospect theory by suggesting that the perception of risks occurs prior to behavior. Based on prospect theory, people perceive losses greater than gains, and hence, the perception of risks is higher in negative framing (which involves losses) than positive framing (which involves gains).

H1: Risk perception is higher in negative framing than positive framing.

Several researchers replicated Tversky and Kahneman's "Asian disease problem" study to extend prospect theory. Levin et al. (1990) found that different amounts of evidence in the Asian Disease problem affected decision-making. In fact, "1 out of 100 people will die" was found to be less trustable than "100 out of 10000 people will die" because the former might be considered a contingency whereas the latter represents a more reliable probability of death. Wang and Johnston (1995) further extended the "Asian Disease Problem" study by varying the number of people (6, 60, 600 and 6000) in

both gain and loss conditions. Their results revealed that under small base size conditions (i.e., 2 out of 6 people live and 20 out of 60 people live), participants tended to be more risk seeking than those who were presented with the large base size conditions (200 out of 600 people live and 2000 out of 6000 people live). Hence, the following hypothesis is proposed.

H2: The greater the base size, the higher the perceived risk.

The findings from Wang and Johnston's (1995) study provide further evidence on how base size influences the effect of framing. Their results demonstrate that base size interacts with framing effects to influence risk-taking behavior. When the base size was 6 and 60, the percentages of subjects who chose the risky option in negative and positive framing were very similar (64% and 70% respectively for base size of 6 and 68% and 65% respectively for base size of 60) but the difference between negative and positive framing increases with larger base sizes. In the larger base size conditions (600 and 6000), the framing effect led to more risk-taking decisions in negative framing than positive framing. This effect was stronger in the large base size conditions than the small base size conditions. A possible reason is that subjects valued individuals in a small group context more heavily than individuals in a large group context (Wang, 1996). In other words, in a small base size context, people are able to ignore the irrelevant cue of framing and thus the framing effect does not affect their choices.

According to this extension of Prospect Theory, we hypothesize that risk information is more powerful when it is based on a large base size. As base size increases, the effect of framing on perceived risk becomes stronger. In other words, people's perception of risks in positive and negative framing widens with increased base size.

H3: As base size increases, framing effect on perceived risk becomes stronger.

Theory of Planned Behavior (TPB), Theory of Reasoned Action (TRA), and Technology Acceptance Model (TAM) provide theoretical foundation for us to examine users' behavior on software download. According to these theories, behavioral intention is the key predictor of actual behavior. In turn, behavioral intention is determined by three factors in TPB (i.e., attitude toward the behavior, subjective norm, and perceived behavioral control) and by two factors in TAM (i.e., attitude toward using and perceived usefulness). In the TPB/TRA model, attitude is one of the key determinants of behavioral intention and addresses the way people feel about a particular behavior. Attitudes are influenced by behavioral beliefs and evaluation of the behavioral outcome, and attitudes refer to one's judgment about whether it is good/safe or bad/dangerous to perform a behavior. In the computer security context, where the particular download behavior is associated with computer security risks, the download intention is the key predictor of the download decision. In other words, the stronger the intention to engage in the download behavior, the more likely the user will make the decision to perform the download action.

Moreover, the download intention is affected by users' attitude toward downloading the software, and perceived risk refers to users' attitude regarding the download behavior. We thus hypothesize that the higher the perceived risk, the lower the behavioral download intention, which in turn, decreases the likelihood of performing the download behavior.

H4: The greater the perceived risk, the lower the download intention.

H5: Download intention is positively associated with the download decision.

Stimulus-Response theory of behavior deals with people's response to a stimulus. Psychologists increasingly question the view that human behavior cannot be completely

explained without taking the internal/mental processes into consideration. The Stimulus-Organism-Response (SOR) theory (Woodworth, 1918), as an extension of the Stimuli-Response formula, suggests that a stimulus may arouse different behavior or response depending on the state of the "organism". The "organism" mediates the relationship between the stimulus and the human's behavior. Basically, the stimulus elicits human's behavior based on a mental process of people. SOR theory has been applied successfully in the IS field to explain customer behavior in the e-commerce context and on social media usage (Jeong et al., 2009). It also provides a lucid outline to study how the framing of a risky scenario influences users' download intention and decision. Thus, the SOR model can work as an overarching framework in this study.

Drawing on SOR Theory, Prospect Theory, TBA, TPB, and TAM, five hypotheses have been generated and the research model is shown in Figure 3.4. Framing and base size of risk information act as the external stimuli that influence users' perceived risk, which further influences users' download intention and behavior, which refer to the response due to the stimuli.

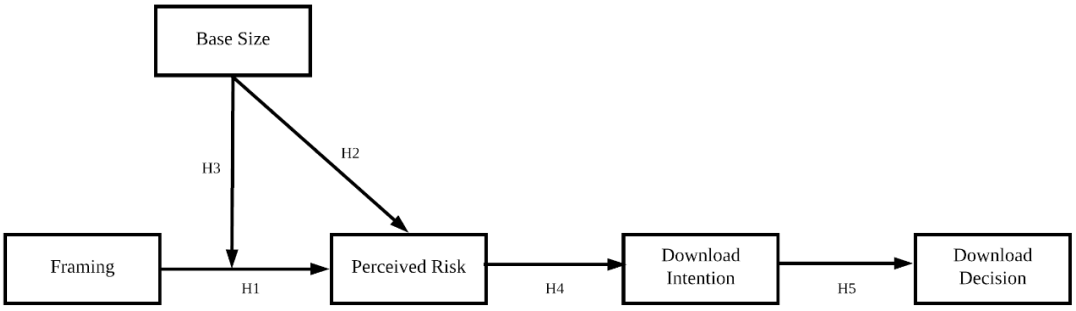

Figure 3.4. Research Model

4. RESEARCH METHODOLOGY

A 2 (positive/negative framing) × 3 (small, medium and large base size) mixed factorial experimental design was conducted to explore the relationship of framing and base size of computer security risk information on users' behavior.

4.1. SUBJECTS

Research subjects were recruited through the crowdsourcing website, Amazon Mechanical Turk (MTurk). Basically, anyone can complete the tasks on the Amazon Mechanical Turk website. The only requirement to carry out the tasks on the Internet and collect payment from the requester is to be at least 18 years of age.

4.2. RESEARCH PROCEDURES

We used a scenario-based survey embedded in an experiment to study users' download behavior. An online survey containing the stimuli in the form of a questionnaire was distributed. Subjects were asked to assess five software download scenarios of which three of them were the experimental stimuli and two of them were distractors, as mentioned earlier.

The software application in each of the three "within-subjects" scenarios was associated with a particular computer security risk, i.e., 10% of those who downloaded the software had their computers infected with viruses, while they differ in their base size (i.e., number of people who downloaded the software).

We detailed the scenario as a free download of an expensive software in order to assess the trade-off between risk and money. In order to eliminate the influence of the

value, type, and importance of one's personal computer (e.g., important data stored in the computer, personal attachment to the computer, etc.), we narrated the situation as follows, which is also presented in Appendix A:

> *"You just bought a new personal computer and have not installed any software or stored any file or information on it. You need to install 5 software applications for a project.*
>
> *Next, you will be given a series of scenarios. Each scenario is related to downloading 1 of the 5 software applications. Each of the scenarios is standalone and independent of one another."*

Then, subjects were provided with different manipulations of a message related to the computer security risk associated with the download. After reviewing each message, subjects needed to respond to a series of questions designed to assess their risk perception, intention, and decision.

4.3. VARIABLES AND OPERATIONALIZATION

Framing was operationalized as a between-subjects variable and base size as a within-subjects variable. All the subjects were randomly assigned to one of the two (positive or negative) framing conditions. In each framing condition, subjects made a software download decision for each of three scenarios involving varying base sizes (i.e., small, medium and large). Moreover, two scenarios were added as distractors in order to mask the systematic pattern among the three main scenarios. The five scenarios, which included the three main scenarios for small, medium and large base size and the two scenarios serving as distractors, were presented to the subjects in a completely randomized order.

4.3.1. Framing. Framing was first studied based on the Asian disease problem, also referred to as "framing of the options". Later on, researchers discussed and explored other types of framing manipulations, such as attribute framing and goal framing (Levin et al., 1998). As an example of attribute framing, a risky situation can be framed by the salience of the outcome including the negative or positive aspects. For example, a download with 10% virus infection rate could be framed in different ways: 9 out of 10 people's computers were secure vs. 1 out of 10 people's computers were infected with viruses. In this study, framing is a between-subjects variable where subjects were randomly assigned to one of the two framing conditions.

In the positive framing condition, the description of the scenarios focused on the positive outcome of downloading the software:

"Among X people who downloaded the software:

Y people's computers were safe and secure"

In the negative framing condition, the scenario focused on the negative outcome of downloading the software:

"Among X people who downloaded the software:

Z person's computer was infected with viruses and crashed unexpectedly"

4.3.2. Base Size. Base size is a within-subjects variable. We manipulated three levels of the base size: 10, 1000, and 100000 (i.e., a difference of 100 times between levels) in order to observe users' perceived risk as base size increased. In order to mask the systematic patterns of the base size manipulations from the subjects, two analogous scenarios (with different computer security risk levels and frequencies) were inserted as distractors. The five scenarios were presented in a randomized order to counter-balance any potential ordering effect.

In the positively framed condition, subjects made download decisions presented in Table 4.1. In the negatively framed condition, subjects made download decisions presented in Table 4.2. The three main scenarios for each of positive and negative framing conditions are also presented in Appendix B.

Table 4.1. Operationalization of Base Size in Positive Framing

Base Size	Paragraph (Positive Framing)
Theta Software (Small Base Size: 10)	Among 10 people who downloaded the software: 9 people's computers were safe and secure
Alpha Software (Medium Base Size: 1,000)	Among 1,000 people who downloaded the software: 900 people's computers were safe and secure
Zeta Software (Large Base Size: 100,000)	Among 100,000 people who downloaded the software: 90,000 people's computers were safe and secure

Table 4.2. Operationalization of Base Size in Negative Framing

Base Size	Paragraph (Negative Framing)
Theta Software (Small Base Size: 10)	Among 10 people who downloaded the software: 1 person's computer was infected with viruses and crashed unexpectedly
Alpha Software (Medium Base Size: 1,000)	Among 1,000 people who downloaded the software: 100 people's computers were infected with viruses and crashed unexpectedly
Zeta Software (Large Base Size: 100,000)	Among 100,000 people who downloaded the software: 10,000 people's computers were infected with viruses and crashed unexpectedly

4.4. MEASUREMENT

After each scenario, a short questionnaire was used to assess perceived risk, download intention, and download decision. The questionnaire also captured Cybersecurity Awareness, Internet Structural Assurance, General Risk-taking Tendencies, Computer Security Risk-taking Tendencies, Self-Efficacy, and the background and demographic information of the subjects. A manipulation check question for framing was presented in the questionnaire. Appendix C and Appendix D present the items in the questionnaire.

4.4.1. Perceived Risk. A three-item scale was developed in this study to assess perceived risk. The first item was adopted from Weber et al. (2002) and the two other items were self-developed. The 5-point Likert scale (not at all risky/no risk at all = 1 to extremely risky/extremely high risk = 5) was used. Table 4.3 shows the items.

Table 4.3. Measurement Scale for Perceived Risk

	Measurement Items
Perceived Risk	(PR1) Please indicate how risky you perceive the action of downloading this software for free from the uncertified source.
	(PR2) Please indicate the level of risk of downloading this software for free from the uncertified source. (Self-developed)
	(PR3) Please rate the riskiness of downloading this software for free from the uncertified source. (Self-developed)

4.4.2. Download Intention. Subjects were asked to rate their intention to download the software. The measurement items for intention were adopted from Ajzen's (1991). The 7-point Likert scale (strongly disagree = 1 to strongly agree = 7) was used. Table 4.4 shows the items.

Table 4.4. Measurement Scale for Download Intention

	Measurement Items
Download Intention	(DI1) I intend to download this software for free from the uncertified source.
	(DI2) I plan to download this software for free from the uncertified source.
	(DI3) It is likely that I will download this software for free from the uncertified source.

4.4.3. Download Decision. After assessing download intention and perceived risk, subjects were asked to answer a question about their download decision:

What is your choice of downloading this software?

- Option 1: Download and pay for the expensive software from the certified source with no security risks
- Option 2: Download the software for free from this uncertified source with the security risks indicated above

4.4.4. General Information Security Awareness. Measurement items were adopted from Bulgurcu et al. (2010) to assess subjects' general information security

awareness. The 7-point Likert scale (strongly disagree = 1 to strongly agree = 7) was used. Table 4.5 presents the items.

Table 4.5. Measurement Scale for General Information Security Awareness

	Measurement Items
General Information Security Awareness	(GISA1) Overall, I am aware of potential security threats and their negative consequences.
	(GISA2) I have sufficient knowledge about the effect of potential security problems. (Revised from original)
	(GISA3) I understand the concerns regarding the risks posed by information security.

4.4.5. Self-Efficacy. The measurement items for self-efficacy were adopted from Dinev and Hu (2007) to assess users' computer security self-efficacy. The 7-point Likert scale (strongly disagree = 1 to strongly agree = 7) was used. Table 4.6 presents the items.

Table 4.6. Measurement Scale for Self-Efficacy

	Measurement Items
Self-Efficacy	(SE1) I am confident that I can remove viruses from my computer.
	(SE2) I am confident that I can prevent unauthorized intrusion into my computer.
	(SE3) I believe I can configure my computer to protect it from viruses.

4.4.6. Cybersecurity Awareness. The measurement items for cybersecurity awareness were adopted from Dinev and Hu (2007). The 7-point Likert scale (strongly disagree = 1 to strongly agree = 7) was used. Table 4.7 presents the items.

Table 4.7. Measurement Scale for Cybersecurity Awareness

	Measurement Items
Cybersecurity Awareness	(CA1) I follow news and developments about virus technology.
	(CA2) I follow news and developments about anti-virus technology. (Revised from original)
	(CA3) I discuss Internet security issues with friends and people around me.
	(CA4) I read about the problems of malicious software intruding into Internet users' computers.
	(CA5) I seek advice from various sources on anti-virus products. (Revised from original)
	(CA6) I am aware of spyware problems and consequences.

4.4.7. Internet Structural Assurance. The measurement items for internet structural assurance were adopted from McKnight et al. (2002) to assess subjects' trust of the Internet. The 7-point Likert scale (strongly disagree = 1 to strongly agree = 7) was used. Table 4.8 presents the items.

4.4.8. General Risk-Taking Tendencies. The measurement items for general risk-taking tendencies were adopted from Meertens and Lion (2008). The 7-point Likert scale (strongly disagree = 1 to strongly agree = 7) was used except for item 6 (see Table 4.9).

Table 4.8. Measurement Scale for Internet Structural Assurance

	Measurement Items
Internet Structural Assurance	(ISA1) The Internet has enough safeguards to make me feel comfortable using it for online transactions.
	(ISA2) I feel assured that legal structures adequately protect me from problems on the Internet. (Revised from original)
	(ISA3) I feel assured that technological structures adequately protect me from problems on the Internet. (Revised from original)
	(ISA4) I feel confident that technological advances on the Internet make it safe for me to carry out online transactions.
	(ISA5) In general, the Internet is a safe environment to carry out online transactions.

Table 4.9. Measurement Scale for General Risk-Taking Tendencies

	Measurement Items
General Risk-taking Tendencies	(GRT1) Safety first. (Reverse coded)
	(GRT2) I prefer to avoid risks. (Reverse coded)
	(GRT3) I take risks regularly.
	(GRT4) I really dislike not knowing what is going to happen. (Reverse coded)
	(GRT5) I enjoy taking risks. (Revised from original)
	(GRT6) In general, I view myself as a ... (Risk avoider = 1 to Risk Seeker = 7)

4.4.9. Computer Security Risk-Taking Tendencies. Based on the measurement items for general risk-taking tendencies from Meertens and Lion (2008), we developed 7 measurement items for computer security risk-taking tendencies. The 7-point Likert scale (strongly disagree = 1 to strongly agree = 7) was used except for item 7 (see Table 4.10).

Table 4.10. Measurement Scale for Computer Security Risk-Taking Tendencies

	Measurement Items
Computer Security Risk-taking Tendencies	(CSRT1) I do not take risks with computer security. (Reverse coded)
	(CSRT2) I generally avoid computer security risks. (Reverse coded)
	(CSRT3) I play it safe with computer security risks. (Reverse coded)
	(CSRT4) I prefer to avoid computer security risks. (Reverse coded)
	(CSRT5) I am not afraid of taking computer security risks.
	(CSRT6) I am willing to take risks with computer security.
	(CSRT7) With regard to computer security, I view myself as a ... (Risk Avoider = 1 to Risk Seeker = 7)

4.4.10. Framing Manipulation Check. The manipulation check question for framing was developed to assess whether the framing manipulation was effective. Subjects were asked to make a selection that comprises two options.

In the previous scenarios, what kind of information was provided? (Please check ALL that apply):

- Option 1: Number of people's computers that were safe and secure
- Option 2: Number of people's computers that were infected with viruses and crashed unexpectedly

4.4.11. Subject Background Questionnaire. The background questionnaire included participants' demographics (e.g., gender, age, education, major) and Internet usage habits (e.g., approximately how many hours do you spend online per week?). Please refer to Appendix D for a complete list of items.

5. DATA ANALYSIS

Subjects were recruited via Amazon's Mechanical Turk (MTurk). In total, 205 people participated in the study, including 75 MTurk master workers and 130 MTurk non-master workers. Among the 205 participants, 8 master workers and 19 non-master workers did not pass the manipulation check question and/or attention check questions. The final sample size of the study is 178 after removing those invalid data points.

We utilized SPSS software to analyze the data collected. This section presents the demographic information of the subjects and the reliability and validity of the measurement. Factor analysis and validity checks on the measurement scales were conducted and the hypotheses were assessed using repeated measures ANOVA and mixed model regression.

5.1. DEMOGRAPHIC INFORMATION OF SUBJECTS

The demographic details of the subjects are summarized in Table 5.1.

Table 5.1. Summary of Demographic Details of Subjects

Gender	
Male	47.8%
Female	52.2%
Age	
18-24	5.1%
25-34	34.3%
35-44	29.8%
45-54	17.4%
55-64	10.1%

Table 5.1. Summary of Demographic Details of Subjects (cont.)

65-74	3.4%
75-84	0.0%
85 or older	0.0%
Race and Ethnicity	
White	70.2%
Black or African American	10.1%
American Indian or Alaskan Native	1.7%
Asian	13.5%
Native Hawaiian or Pacific Islander	0.6%
Other	3.9%
Marital Status	
Married	41.0%
Widowed	0.6%
Divorced	10.1%
Separated	2.8%
Never Married	45.5%
Education Level	
Less than high school degree	0.6%
High school graduate (including GED)	7.9%
Some college but no degree	15.7%
Associate degree in college (2-year)	11.8%
Bachelor's degree in college (4-year)	46.1%
Master's degree	14.6%
Doctoral degree	2.8%
Professional degree (JD, MD)	0.6%
Employment Status	
Employed full time	70.8%
Employed part time	15.7%
Unemployed looking for work	2.8%
Unemployed not looking for work	5.1%
Retired	3.4%
Student	2.2%
Occupation	
Management, professional, and related	46.1%
Sales and office	23%
Farming, fishing, and forestry	6.7%
Government	3.4%
Retired	7.9%
Unemployed	12.9%

Table 5.1. Summary of Demographic Details of Subjects (cont.)

Personal Income (Previous Year, Before Taxes)	
Less than $10,000	13.5%
$10,000 to $29,999	24.2%
$30,000 to $49,999	24.2%
$50,000 to $69,999	18%
$70,000 to $89,999	12.4%
$90,000 to $109,999	2.8%
$110,000 to $129,999	2.8%
$130,000 to $149,999	0.6%
$150,000 or more	1.1%
Prefer not to disclose	0.6%
Family Income (Previous Year, Before Taxes)	
Less than $10,000	6.7%
$10,000 to $49,999	36.5%
$50,000 to $99,999	39.9%
$100,000 to $149,999	10.1%
$150,000 to $199,999	2.8%
$200,000 to $249,999	1.7%
$250,000 or more	1.1%
Prefer not to disclose	1.1%
Disposable Income (Per Month)	
Less Than $100	20.8%
$100 - $500	38.8%
$501 - $1000	19.1%
$1001 - $2000	14.6%
More Than $2000	6.7%
Time Spent Online (Per Week)	
1-5 hours	3.9%
6 - 10 hours	12.9%
11-15 hours	13.5%
16-20 hours	14.6%
20+ hours	55.1%
Frequency of Software Download from Unknown Sources	
Never	50.0%
Sometimes	43.3%
About half of the time	2.8%
Most of the time	3.4%
Always	0.6%

5.2. MEASUREMENT VALIDATION

To evaluate convergent and discriminant validity for the constructs in the questionnaire, exploratory factor analysis (EFA) was carried out. The EFA results using Varimax Rotation and Principal Component Analysis are shown in Table 5.2. An eight-factor structure was generated with eigenvalues greater than 1.0.

Table 5.2. Results of Exploratory Factor Analysis (with all measurements)

	Component							
	1	2	3	4	5	6	7	8
DI1_L	0.878	-0.225	0.202	-0.027	0.075	-0.047	0.120	-0.185
DI3_L	0.874	-0.228	0.180	-0.008	0.079	-0.069	0.109	-0.211
DI2_L	0.871	-0.251	0.174	0.023	0.068	-0.048	0.124	-0.179
DI2_M	0.857	-0.297	0.235	0.084	0.100	0.022	0.114	-0.021
DI1_M	0.850	-0.316	0.243	0.062	0.096	0.043	0.152	0.004
DI1_S	0.841	-0.326	0.238	0.088	0.099	0.009	0.041	0.141
DI3_M	0.840	-0.307	0.241	0.090	0.073	0.034	0.127	0.029
DI3_S	0.833	-0.331	0.196	0.116	0.095	0.001	0.017	0.147
DI2_S	0.821	-0.359	0.219	0.062	0.089	-0.016	0.050	0.165
PR3_S	-0.197	0.895	-0.120	0.014	-0.089	-0.018	-0.041	-0.162
PR1_S	-0.231	0.879	-0.147	-0.004	-0.112	-0.022	-0.038	-0.206
PR2_S	-0.259	0.868	-0.112	0.003	-0.121	-0.020	0.007	-0.178
PR1_M	-0.316	0.857	-0.135	-0.011	-0.148	0.029	-0.080	0.072
PR2_M	-0.285	0.854	-0.144	-0.059	-0.076	0.044	-0.096	0.017
PR3_M	-0.263	0.842	-0.134	-0.060	-0.069	0.050	-0.105	0.079
PR1_L	-0.316	0.760	-0.114	0.103	-0.121	0.097	-0.049	0.429
PR3_L	-0.318	0.733	-0.156	0.125	-0.139	0.052	-0.084	0.455
PR2_L	-0.309	0.708	-0.140	0.055	-0.131	0.089	-0.064	0.468
GRT5	0.108	-0.132	0.845	-0.016	-0.050	0.174	-0.021	0.031
GRT6	0.301	-0.097	0.823	-0.037	-0.010	0.066	-0.013	0.007
GRT3	0.226	-0.151	0.810	0.112	0.057	0.148	0.036	0.050

Table 5.2. Results of Exploratory Factor Analysis (with all measurements) (cont.)

GRT2	0.274	-0.120	0.785	0.089	0.073	-0.029	0.133	-0.071
GRT4	0.024	-0.102	0.685	0.029	0.158	-0.022	0.054	-0.010
GRT1	0.289	-0.185	0.660	-0.001	0.035	-0.149	0.297	-0.100
SE3	0.138	-0.056	0.088	0.804	0.141	0.079	0.000	0.156
SE1	0.311	-0.066	0.182	0.743	0.151	0.000	0.036	0.090
SE2	0.185	-0.027	0.055	0.716	0.287	0.086	0.053	0.213
GISA2	0.033	-0.056	0.019	0.768	0.090	0.243	-0.005	-0.075
GISA1	-0.221	-0.017	-0.083	0.658	0.125	0.327	-0.050	-0.252
GISA3	-0.077	0.218	-0.051	0.652	0.083	0.291	-0.340	-0.172
ISA4	0.127	-0.111	0.025	0.154	0.811	0.044	0.014	-0.001
ISA3	0.246	-0.114	0.043	0.118	0.791	-0.060	0.046	0.022
ISA1	0.018	-0.127	0.091	0.164	0.786	-0.064	0.080	-0.112
ISA5	-0.105	-0.150	0.066	0.225	0.692	0.094	0.130	-0.090
ISA2	0.349	-0.134	0.184	-0.004	0.671	0.127	-0.123	0.214
CA1	-0.073	-0.039	0.081	0.244	0.036	0.816	0.146	0.099
CA2	-0.035	-0.005	0.050	0.238	0.012	0.815	0.195	0.097
CA3	0.065	-0.001	0.023	0.089	0.051	0.712	-0.157	0.005
CA5	-0.016	0.094	0.085	0.116	-0.032	0.67	-0.159	-0.216
CA4	0.013	0.089	-0.036	0.370	0.003	0.571	-0.102	0.091
CA6	-0.134	0.125	-0.149	0.702	0.011	0.335	-0.034	-0.067
CSRT2	0.410	-0.138	0.519	-0.110	0.081	-0.093	0.587	-0.111
CSRT3	0.450	-0.114	0.421	-0.176	0.073	-0.162	0.575	0.030
CSRT6	0.401	-0.199	0.482	-0.009	0.131	0.068	0.557	0.031
CSRT4	0.471	-0.134	0.423	-0.083	0.114	-0.130	0.513	-0.057
CSRT1	0.436	-0.152	0.436	-0.016	0.163	0.012	0.472	0.013
CSRT5	0.377	-0.167	0.550	0.023	0.103	0.057	0.311	-0.084
CSRT7	0.554	-0.015	0.595	-0.051	0.103	-0.019	0.218	0.122

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 7 iterations.

As shown in Table 5.2, Self-Efficacy (SE) and General Information Security Awareness (GISA) load together. In reviewing the items for GISA, it is noted that they tapped on knowledge and awareness of information security, and hence, are very similar to SE. Since there is another measurement for computer security awareness (i.e., Cybersecurity Awareness (CA)) that was assessed based on actions and behavior associated with awareness of cybersecurity, all items of GISA were dropped while those of CA were retained. However, since item CA6 did not load well, it was removed. In addition, Computer Security Risk-Taking Tendencies (CSRT) loaded with General Risk-Taking Tendencies (GRT), and hence, we decided to retain GRT and discard CSRT. The rest of the measurement items loaded onto their target factors, which suggests good construct validity (Cook, et al., 1979).

After removing construct GISA, CSRT, and item CA6, we ran the factor analysis again. Table 5.3 provides the results of EFA after the adjustments.

Table 5.3. Results of Factor Analysis (after removing GISA, CSRT, and CA6)

	Component					
	1	2	3	4	5	6
DI1_L	0.892	-0.250	0.187	0.093	-0.058	-0.028
DI3_L	0.887	-0.254	0.166	0.102	-0.075	-0.019
DI2_L	0.883	-0.272	0.166	0.090	-0.053	0.021
DI2_M	0.863	-0.305	0.220	0.110	0.027	0.115
DI1_M	0.857	-0.325	0.229	0.102	0.044	0.115
DI1_S	0.845	-0.312	0.223	0.080	0.040	0.138
DI3_M	0.840	-0.315	0.217	0.096	0.013	0.165
DI3_S	0.827	-0.319	0.171	0.091	0.009	0.191
DI2_S	0.819	-0.346	0.203	0.080	-0.013	0.166

Table 5.3. Results of Factor Analysis (after removing GISA, CSRT, and CA6) (cont.)

PR3_S	-0.186	0.884	-0.104	-0.064	-0.016	-0.080
PR1_S	-0.312	0.864	-0.128	-0.149	0.025	-0.050
PR2_S	-0.219	0.863	-0.129	-0.086	-0.022	-0.113
PR2_M	-0.277	0.859	-0.135	-0.074	0.032	-0.113
PR1_M	-0.245	0.854	-0.089	-0.096	-0.018	-0.093
PR3_M	-0.259	0.852	-0.123	-0.074	0.040	-0.092
PR1_L	-0.320	0.801	-0.105	-0.148	0.103	0.163
PR3_L	-0.327	0.780	-0.147	-0.165	0.066	0.191
PR2_L	-0.314	0.754	-0.129	-0.162	0.091	0.135
GRT5	0.130	-0.129	0.835	-0.040	0.170	-0.029
GRT3	0.246	-0.145	0.803	0.074	0.155	0.113
GRT6	0.310	-0.108	0.800	-0.006	0.075	0.012
GRT2	0.299	-0.129	0.792	0.096	-0.013	0.100
GRT1	0.324	-0.201	0.700	0.065	-0.157	0.029
GRT4	0.043	-0.105	0.690	0.166	-0.018	0.044
ISA4	0.121	-0.107	0.022	0.819	0.057	0.125
ISA1	0.026	-0.133	0.088	0.808	-0.060	0.089
ISA3	0.237	-0.119	0.022	0.789	-0.051	0.131
ISA5	-0.099	-0.152	0.079	0.717	0.108	0.155
ISA2	0.327	-0.129	0.122	0.634	0.123	0.078
CA1	-0.056	-0.016	0.123	0.058	0.831	0.146
CA2	-0.014	0.016	0.099	0.039	0.826	0.134
CA3	0.048	-0.003	-0.020	0.049	0.736	0.011
CA5	-0.033	0.064	0.033	-0.015	0.706	-0.026
CA4	-0.008	0.105	-0.054	0.011	0.625	0.305
SE3	0.096	-0.031	0.064	0.165	0.205	0.847
SE1	0.274	-0.053	0.155	0.182	0.122	0.786
SE2	0.140	-0.011	0.017	0.302	0.204	0.777

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 7 iterations.

Cronbach's alpha coefficients of at least 0.70 indicate good reliability of the constructs (Nunnally et al., 1967). All of the Cronbach's alpha coefficients shown in Table 5.4 are above 0.7, suggesting that all the measures and their respective measurement components are reliable.

Table 5.4. Results of Reliability Analysis

Variable	Cronbach's Alpha
Download Intention (DI) (3 items)	0.986
Perceived Risk (PR) (3 items)	0.972
Self-Efficacy (SE) (3 items)	0.870
Cybersecurity Awareness (CA) (5 items)	0.819
Internet Structural Assurance (ISA) (5 items)	0.848
General Risk-Taking Tendencies (GRT) (6 items)	0.899

5.3. REPEATED MEASURES ANALYSIS OF VARIANCE

Repeated measures refer to measures that are repeated with the same subject. Repeated measures analysis of variance (ANOVA) is also referred to as within-subjects ANOVA. Repeated measures ANOVA is used to assess overall differences between related means differences in mean scores for two or more within-subjects conditions. Moreover, it is appropriate to use a repeated measures ANOVA only if the data "passes" five assumptions (Field, 2009).

1. The dependent variable should be measured at the continuous level (i.e., interval or ratio scale; ordinal scale is also acceptable).

2. The within-subjects variable should consist of at least two levels.
3. There should be no significant outliers in the related groups. The problem with outliers is that they might have a negative effect on the repeated measures ANOVA, distorting the differences between the related groups (whether increasing or decreasing the scores on the dependent variable), and can reduce the accuracy of the results.
4. The distribution of the dependent variable in the two or more related groups should be approximately normally distributed. However, this assumption is not needed if the sample size is greater than 25.
5. The variances of the differences between all combinations of related groups should be equal or approximately equal.

5.3.1. Check for Assumptions. The sample size of this study is 178. Base Size is the within-subjects variable that has three levels (small, medium and large); framing is the between-subjects factor with two levels (positive and negative); and the outcome or dependent factor is perceived risk which is measured at the continuous level (i.e., ordinal scale can be approximated to be continuous). Thus, the data meet assumptions 1, 2, and 4.

To test assumptions 3, we ran analyses in SPSS to detect possible outliers at each level of the repeated measures in our data. The results of outlier detection are provided in Figure 5.1-5.3.

SPSS makes a distinction between outliers that are more than 1.5 box lengths from one hinge of the box (using a circle) and outliers that are more than 3 box lengths from a hinge (using an asterisk). Based on an examination of the boxplots, SPSS does not identify any outliers since there is no circle or asterisk in Figures 5.1-5.3. Thus, our data meet assumption 3 of Repeated Measures ANOVA.

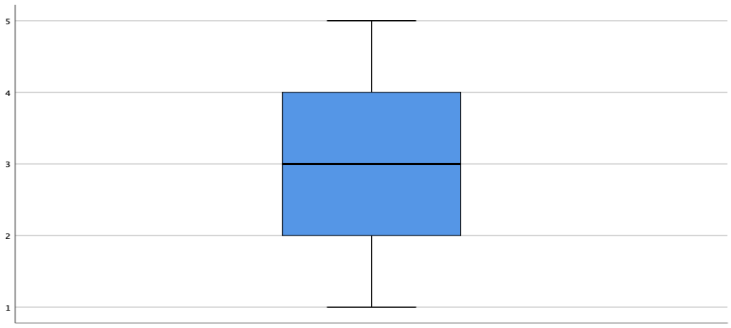

Figure 5.1. SPSS Explore Output: Boxplot for Perceived Risk in Small Base Size

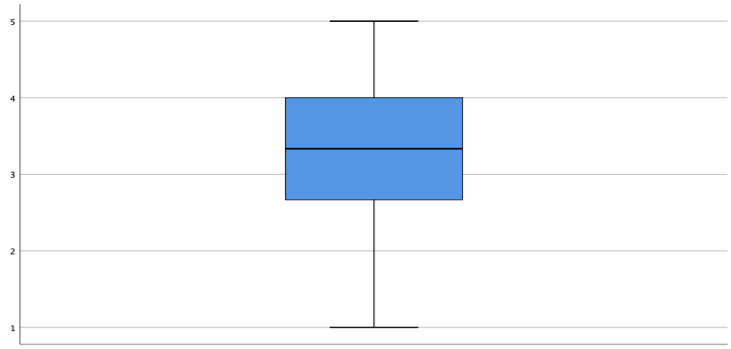

Figure 5.2. SPSS Explore Output: Boxplot for Perceived Risk in Medium Base Size

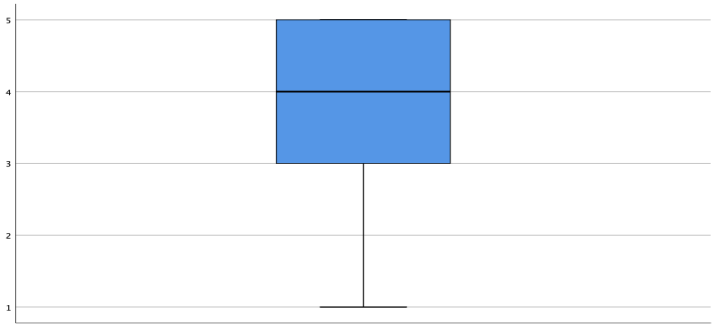

Figure 5.3. SPSS Explore Output: Boxplot for Perceived Risk in Large Base Size

Assumption 5 requires the variances of the differences between all combinations of related groups to be equal (i.e., Sphericity). Sphericity is tested with the Mauchly's test (Mauchly, 1940). When the probability of Mauchly's test is greater than α (i.e., $p > 0.05$ with α usually set to 0.05), the variances are equal and thus sphericity has not been violated. Since the results of Mauchly's test of our data show that sphericity is violated (i.e., $p < 0.05$), we use alternatives ways for estimating the amount of sphericity. In SPSS, three alternative methods are also generated: Greenhouse-Geisser, Huynh-Feldt, and the lower-bound (Greenhouse & Geisser, 1959; Huynh & Feldt, 1976). If Mauchly's test of sphericity is violated, these methods are used to correct the within-subjects tests. The Greenhouse-Geisser and Huynd-Feldt corrections estimate ε in order to correct the degrees of freedom of the F-distribution. These corrections have elicited a more accurate significance value as they increase the *p*-value to compensate for the fact that the test is too liberal when sphericity is violated. Moreover, the Greenhouse-Geisser correction tends to underestimate ε when ε is close to 1 and thus it is a conservative correction, whereas the Huynd-Feldt correction tends to overestimate ε so it is a more liberal correction.

5.3.2. Results of Repeated Measures ANOVA. Given that there is a within-subjects factor (base size) and a between-subjects factor (framing) in the research design, we used the repeated measures ANOVA for testing H1, H2 and H3.

5.3.2.1. Tests of between-subjects effects (framing). Section 5.3.2.1 presents the results of the main effect of Framing, a between-subjects factor. Table 5.5 shows the descriptive statistics for the effect of Positive and Negative Framing on Perceived Risk. As shown in Table 5.5, the mean for Perceived Risk is higher in Negative Framing than

for Positive Framing. Figure 5.4 shows a diagram of the main effect of framing across all three levels of base size in negative framing and positive framing.

Table 5.5. Descriptive Statistics of Between-Subjects Effects for Framing

Framing	Mean	Std. Deviation	95% Confidence Interval	
			Lower Bound	Upper Bound
Negative	3.83	1.02	3.63	4.03
Positive	3.10	1.08	2.91	3.30

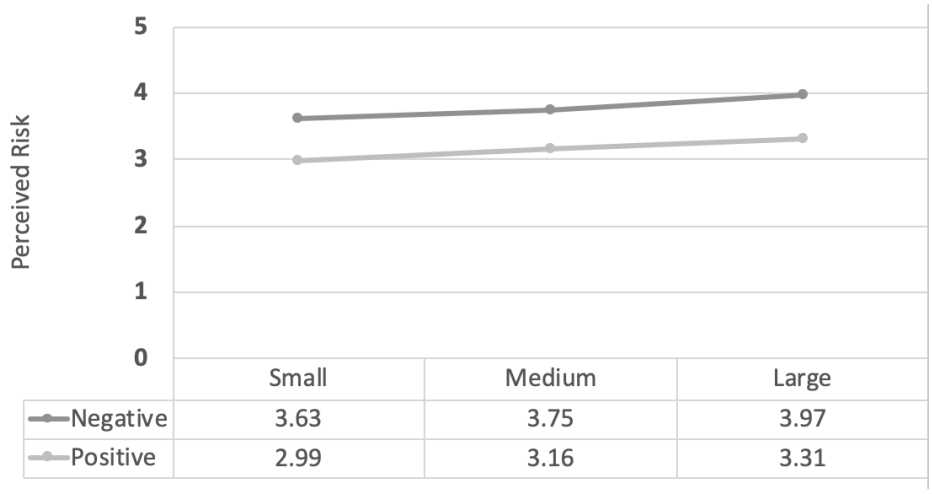

Figure 5.4. Main Effect of Framing Across Three Levels of Base Size

In addition, Table 5.6 shows the results of the Framing main effect on Perceived Risk, along with 17 covariates in the following three categories:

- Demographic Factors (10): Gender, Age, Ethnicity, Marital Status, Education, Employment Status, Occupation, Annual Personal Income, Annual Household Income, and Disposable Income or Allowance.
- Computer Usage (2): Hours Spent Online Per Week, Frequency of Download Software from Unknown Sources.
- Individual Traits (4): Internet Structural Assurance, General Risk-Taking Tendencies, Cybersecurity Awareness, and Self-Efficacy.

In Table 5.6, **Sum of Squares** is the sum of the squares of the deviations from the means. Degree of Freedom (**df**) represents the degree of freedom of the coefficients for the test. **Mean Square** is found by dividing the Sum of Squares by the Degree of Freedom. **F** refers to the ratio of two independent chi-squared variables divided by their respective degrees of freedom. **Sig.** refers to the 2-tailed p-value to test if the value of the null hypothesis is 0. For our data analysis, we compared each *p*-value to our preselected alpha threshold of 0.05. Coefficients that have a *p*-value less than the preselected alpha value is considered to be statistically significant.

Framing. We found that framing has a significant effect on Perceived Risk, $p < 0.001$. Subjects who were in Negative Framing exhibited greater Perceived Risk than those in Positive Framing (Mean = 3.83, SD = 1.08) than subjects who were in Positive Framing (Mean = 3.10, SD = 1.02). Hence, H1 is supported.

Internet Structural Assurance (ISA). We found a significant effect of Internet Structural Assurance on Perceived Risk, $p = 0.004$ (< 0.05). Subjects who are high in ISA perceived lower risks of downloading the software for free from the uncertified source.

General Risk-Taking Tendencies (GRT). We found a significant effect of General Risk-Taking Tendencies on Perceived Risk, $p < 0.001$. Subjects who are high in General

Risk-Taking Tendencies perceived lower risks of downloading the software for free from the uncertified source.

Table 5.6. Tests of Between-Subjects Effects

Source	Sum of Squares	df	Mean Square	F	Sig. (2-tailed)
Intercept	89.33	1	89.33	43.71	0.000
Framing	49.90	1	49.9	24.42	**0.000**
Self-Efficacy	0.47	1	0.47	0.23	0.632
Cybersecurity Awareness	1.72	1	1.72	0.84	0.361
Internet Structural Assurance	16.60	1	16.60	8.12	**0.005**
General Risk-Taking Tendencies	31.93	1	31.93	15.62	**0.000**
Gender	0.85	1	0.85	0.41	0.521
Age	4.92	1	4.92	2.41	0.123
Ethnicity	13.36	1	13.36	6.54	**0.012**
Marital Status	0.60	1	0.60	0.29	0.589
Degree	0.98	1	0.98	0.48	0.489
Employment Status	7.35	1	7.35	3.60	0.060
Occupation	0.00	1	0.00	0.00	0.974
Personal Income	0.19	1	0.19	0.09	0.763
Household Income	0.76	1	0.76	0.37	0.543
Disposable Income	15.03	1	15.03	7.36	**0.007**
Hour Spent Online	0.47	1	0.47	0.23	0.633
Frequency of Download Software from Unknown Sources	4.47	1	4.47	2.19	0.141

All other covariates with the exception of disposable income and ethnicity are not significant. Disposable income and ethnicity have effects on perceived risk of users. People who have the lowest and highest disposable income brackets perceived the lightest risks. Since we have a large number of white subjects (70%), we compared them with the rest of the subjects and found a difference in their risk perceptions.

5.3.2.2. Tests of within-subjects effects (base size). In this section, Table 5.7 provides the descriptive statistics and shows the means for Perceived Risk at the different levels of Base Size and Framing. Table 5.8 shows the results of repeated measures ANOVA which indicates the overall significance of the within-subjects effect of Base Size and the interaction effect of Framing and Base Size. As mentioned in Section 5.3.1, since our data violate the assumption of sphericity (i.e., equal variances), we use the values of the "Greenhouse-Geisser" test instead of "Sphericity Assumed".

Table 5.7. Descriptive Statistics for Perceived Risk at Three Levels of Base Size

Base Size	Mean	Std. Deviation	95% Confidence Interval		Framing	Mean	Std. Deviation
			Lower Bound	Upper Bound			
Small	3.31	1.15	3.15	3.47	Negative	3.68	1.08
					Positive	2.94	1.10
					Total	3.31	1.15
Medium	3.45	1.07	3.30	3.60	Negative	3.80	0.99
					Positive	3.10	1.04
					Total	3.45	1.07
Large	3.64	1.09	3.49	3.79	Negative	4.01	0.97
					Positive	3.27	1.08
					Total	3.64	1.09

Table 5.8. Tests of Within-Subjects Effects of Base Size

Source		Sum of Squares	df	Mean Square	F	Sig.
Base Size	Sphericity Assumed	9.73	2.00	4.86	17.07	0.00
	Greenhouse-Geisser	9.73	1.76	5.53	17.07	0.00
	Huynh-Feldt	9.73	1.79	5.44	17.07	0.00
	Lower-bound	9.73	1.00	9.73	17.07	0.00
Framing * Base Size	Sphericity Assumed	0.04	2.00	0.02	0.07	0.93
	Greenhouse-Geisser	0.04	1.76	0.02	0.07	0.91
	Huynh-Feldt	0.04	1.79	0.02	0.07	0.91
	Lower-bound	0.04	1.00	0.04	0.07	0.79
Error (Base Size)	Sphericity Assumed	100.31	352.00	0.29		
	Greenhouse-Geisser	100.31	309.88	0.32		
	Huynh-Feldt	100.31	314.55	0.32		
	Lower-bound	100.31	176	0.57		

Base size. According to the results of repeated measures ANOVA with a Greenhouse-Geisser correction presented in Table 5.7, the mean scores for Perceived Risk are statistically different ($p < 0.001$) between the different levels of Base Size. The results illustrate that subjects perceived greater risk (Mean = 3.64, SD = 1.09) when provided the scenario with large base size than with small base size (Mean = 3.31, SD = 1.15) and medium base size (Mean = 3.45, SD = 1.07). Since the overall ANOVA results for the three levels of base size are significant, we also ran the post-hoc tests to see which levels of Base Size are different. According to the post-hoc tests presented in Table 5.9, there is a significant effect across every level of Base Size on Perceived Risk. We can see that there is a significant difference in Perceived Risk between small and medium Base

Size ($p = 0.01 < 0.05$, MD = 0.14), between small and large Base Size ($p < 0.001$, MD = 0.33), and between medium and large Base Size ($p < 0.001$, MD = 0.19). From the Mean Difference column, we can see that as the Base Size increases, Perceived Risk is also significantly increased. Hence, H2 is supported.

Table 5.9. Results of the Bonferroni Post-Hoc Tests

Base Size		Mean Difference	Std. Error	Sig.	95% Confidence Interval for Difference	
					Lower Bound	Upper Bound
Small	**Medium**	-0.14	0.05	0.01	-0.24	-0.04
	Large	-0.33	0.07	0.00	-0.46	-0.20
Medium	**Small**	0.14	0.05	0.01	0.04	0.24
	Large	-0.19	0.05	0.00	-0.29	-0.09
Large	**Small**	0.33	0.07	0.00	0.20	0.46
	Medium	0.19	0.05	0.00	0.09	0.29

Framing*Base Size. According to the results of repeated measures ANOVA with a Greenhouse-Geisser correction presented in Table 5.7, there is no interaction effect between Framing and Base Size on Perceived Risk ($p = 0.909 > 0.05$). Hence, H3 is not supported.

5.4. MIXED MODEL REGRESSION ANALYSIS

We measured Perceived Risk, Download Intention, and Download Decision as repeated measures at small, medium, and large levels of base size in the study. As Repeated Measures ANOVA can only treat a repeated measures as a categorical factor, we conducted Mixed Model Regression Analysis to test H4 and H5.

A mixed model is a statistical model containing both fixed effects and random effects. They are particularly useful in settings where repeated measurements are made on the same statistical units (longitudinal study), or where measurements are made on clusters of related statistical units (Lindstrom & Bates, 1990). In the Mixed Model approach, each subject has three rows of data. A new column is generated to indicate the level of Base Size and the outcomes (i.e., Perceived Risk, Download Intention, and Download Decision) are single variables. Covariates have repeated values across the three rows of data. This is called the long format, or Stacked data, and this changes the unit of analysis from the subject to each measurement occasion.

The results of Mixed Model Regression Analysis for Download Intention are presented in Table 5.10, and the results of Mixed Model Regression Analysis for Download Decision are presented in Table 5.11.

Table 5.10. Tests of Perceived Risk Effects on Download Decision

Source	Numerator df	Denominator df	F	Sig.
Intercept	1	463.72	363.30	0.00
Perceived Risk	12	403.64	25.64	0.00
a. Dependent Variable: Download Intention.				

Download Intention. From the result of the analysis as shown in Table 5.10, we found a significant effect of Perceived Risk on Download Intention, $p < 0.001$. Subjects who perceived greater risks have lower download intentions. Hence, H4 is supported.

Table 5.11. Tests of Download Intention Effects on Download Behavior

Source	Numerator df	Denominator df	F	Sig.
Intercept	1	411.36	3612.96	0.00
Download Intention	18	436.36	62.32	0.00
a. Dependent Variable: Download Decision.				

Download Decision. From the result of the analysis as shown in Table 5.11, we found a significant effect of Download Intention on Download Decision, $p < 0.001$. Download intentions are positively associated with download decisions. Hence, H5 is supported.

Table 5.12 summarizes the results of hypothesis testing. In sum, H1, H2, H4, and H5 are supported but H3 is not supported. The next section discusses the findings.

Table 5.12. Results of Hypothesis Testing

Hypothesis	Supported?
H1: Risk perception is higher in negative framing than positive framing.	Yes
H2: The greater the base size, the higher the perceived risk.	Yes
H3: As base size increases, framing effect on perceived risk becomes stronger.	No
H4: The greater the perceived risk, the lower the download intention.	Yes
H5: Download intention is positively associated with download decision.	Yes

6. DISCUSSIONS

The results of our study provide further evidence to the literature that framing influences users' perceptions of risks. In addition, the results demonstrate that base size, manipulated through the number of people who downloaded the software, influences users' perceived risks. However, the results do not demonstrate the interaction effect of base size and framing on users' behavior found by Wang and Johnston (1995) as the framing effect in our study is consistent across all base size conditions. Hence, based on our study, base size does not moderate the effect of framing on perceived risk. The findings also suggest that users' perceived risk has a significant effect on users' download intention, and users' download intention is positively associated with users' download decision.

First, negative framing leads to higher perceived risk than positive framing. According to Prospect Theory, a loss is assessed at a relatively greater value than a gain. The finding is in line with Prospect Theory and suggests that users' perception of computer security risk is higher in the negative framing condition than in the positive framing condition.

Second, base size has a significant impact on users' perceived risk. The larger the base size, the greater the perceived risk. As base size increases, the perceived probability of virus infection increases and thus, users' perceived risk increases.

Moreover, the results have shown that the greater the perceived risk, the lower the intention to download software applications that involve computer security risks. Hence, providing computer security risk information with negative framing is an effective way to reduce or minimize computer security risk-taking behavior.

Hence, users are less likely to download software applications when the risk information is framed negatively and when the risk information is presented with a large base size.

7. LIMITATIONS AND FUTURE RESEARCH

The study has several limitations, which can be resolved or addressed in future research.

First, the data collection of this study was conducted on MTurk to ensure a diverse sample across different age groups, ethnicity, occupation, etc. However, MTurk does not operate in a controlled environment, thus we cannot ensure subjects were focused and not distracted by interference in their surroundings during the study. In future research, we would like to recruit subjects to participate in a controlled laboratory experiment to validate the results.

Second, the study utilized a scenario-based survey approach to manipulate the experimental scenarios. It did not simulate any actual uncertified software downloads which could have made the experimental scenarios more realistic. This limitation could be overcome in future research by simulating more realistic-looking websites involving decisions on uncertified software downloads and hence, make the experimental conditions look more realistic or similar to those encountered in real life.

Third, many participants felt that the questionnaire is a bit long as we have a large number of demographic questions. We intended to use the demographic items as covariates in our study, so we used a fairly comprehensive set of subject demographic questions. However, since demographic questions are generally straight-forward to answer (i.e., do not require much thought or cognitive processing to answer them), we placed them at the end of the questionnaire because errors due to fatigue were less likely to happen for demographic questions compared to other types of questions. Furthermore, we included attention check questions and eliminated data points that were problematic

due to lack of attention by the subjects. Future studies can overcome this potential limitation by further refining the demographic items.

Fourth, we captured and analyzed only a few traits such as cybersecurity awareness, self-efficacy, and risk-taking tendencies. In future research, other personality traits such as the big five factors of personality could also be studied.

8. CONCLUSIONS

This research examines the impact of positively and negatively framed security risk information and base size on computer security risk perceptions of users. It also investigates the relationship between risk perceptions and download intentions, as well as download intentions and download decisions. In addition, it examines the effects of various demographic factors and personality traits on perceived risks, e.g., gender, age, cybersecurity awareness, internet structural assurance, and risk-taking tendencies.

Our findings are significant because negative framing is indeed the way computer security risks should be presented to decision makers. Drawing on Prospect Theory, this study focuses on understanding whether negatively framed cybersecurity risk information could lead users to engage in less risk-taking or more conservative online behavior as compared to positively framed cybersecurity risk information. The findings suggest that the framing of risk information has a significant effect on users' behavior. More specifically, negative framing increases users' perceived risk, leading to risk-averse behavior, which is consistent with Prospect Theory in that people weigh losses greater than gains of the same amount or magnitude.

The experimental conditions of our study are different other studies on framing effect and decision-making in information science context (Beebe et al., 2014, Rosoff et al., 2013, and Valecha et al., 2016). Our study presented one situation with two different frames, i.e., negatively framed scenario vs. positively framed scenario, whereas their studies provided two opposite scenarios, which are gain vs. loss or reward-based phishing email vs. threat-based phishing email. Moreover, our results are different from the results of Chen et al., (2015), which suggest that positive framing decreases risk-taking behavior.

Their study provides two conditions: the amount of safety and the amount of risks of an app installation. However, safety differs from risks because safety seems to be an integrated concept and people rarely talk about the dimensions for safety, but risk is a multi-dimension concept that generally is regarded to comprise three dimensions: probability, assets, and consequences. Thus, people may tend to think of overall safety but components of risks. The positive/negative framing in our study seems to be balanced as we provided two conditions that are logically opposite to each other: among a group of people, the number of people's computers that were infected with viruses vs. the number of people's computers that were secure.

This study also explores the base size effect, which supports the idea that people tend to be less risk seeking as base size increases, as discussed by Wang and Johnston (1995), and Levin and Chapman (1990). In our study, the base size effect was found in both positive and negative framing. The results demonstrate that base size affects people's risk perceptions such that the greater the base size, the higher the perceived risk.

Data analysis was also carried out to study the effect of personality traits, such as cybersecurity awareness, general risk-taking tendencies, and Internet structural on users' perceived computer security risk. We found a significant effect of users' perceived Internet structural assurance on perceived risk. Users who have higher internet structural assurance are more likely to perceive less risk of downloading software from uncertified sources. Moreover, there is a negative effect of general risk-taking tendencies on perceived risk. Users with higher general risk-taking tendencies perceive less risks of downloading software from uncertified sources.

In summary, this study offers insights on the impact of framing and base size in the context of computer security. With the knowledge gained from this research, we hope

to design better warning systems to mitigate the risks undertaken by users. The findings from this research study can also be applied to train employees about avoiding dangerous software downloads by presenting training materials more effectively and thereby reducing the chances of employees taking risky computer security actions.

APPENDIX A.

SCENARIO DETAILS

Scenario:

You just bought a new personal computer and have not installed any software or stored any file or information on it. You need to install **5 software applications** for a project.

Next, you will be given a series of scenarios. Each scenario is related to downloading 1 of the 5 software applications. Each of the scenarios is **standalone** and **independent** of one another.

Please click 'Next' to continue.

Next

APPENDIX B.

EXPERIMENTAL CONDITIONS

1. POSITIVELY FRAMED SCENARIO

1.1 Small Base Size

SCENARIO:

You are looking into downloading Theta, an **expensive** software, that you need for a personal project.

Due to the cost of Theta software, you searched online and found an uncertified source that you can download Theta software for **free** with the following security risks:

> Among **10** people who downloaded the software:
> **9** people's computers were **safe and secure**

Hence, you have two options to download the software for the project:

- **Pay Option**: Download and pay for the **expensive** software from the certified source with no security risks
- **Free Option**: Download the software for **free** from this uncertified source with the security risks indicated above

1.2 Medium Base Size

SCENARIO:

You are looking into downloading Alpha, an **expensive** software, that you need for a personal project.

Due to the cost of Alpha software, you searched online and found an uncertified source providing a download of Alpha software for **free** with the following security risks:

> Among **1,000** people who downloaded the software:
> **900** people's computers were **safe and secure**

Hence, you have two options to download the software for the project:

- **Pay Option**: Download and pay for the **expensive** software from the certified source with no security risks
- **Free Option**: Download the software for **free** from this uncertified source with the security risks indicated above

1.3 Large Base Size

SCENARIO:

You are looking into downloading Zeta, an **expensive** software, that you need for a personal project.

Due to the cost of Zeta software, you searched online and found an uncertified source providing a download of Zeta software for **free** with the following security risks:

> Among **100,000** people who downloaded the software:
> **90,000** people's computers were **safe and secure**

Hence, you have two options to download the software for the project:

- **Pay Option**: Download and pay for the **expensive** software from the certified source with no security risks
- **Free Option**: Download the software for **free** from this uncertified source with the security risks indicated above

2. NEGATIVELY FRAMED SCENARIO

2.1 Small Base Size

SCENARIO:

You are looking into downloading Theta, an **expensive** software, that you need for a personal project.

Due to the cost of Theta software, you searched online and found an uncertified source that you can download Theta software for **free** with the following security risks:

> Among **10** people who downloaded the software:
> **1** person's computer was **infected with viruses and crashed unexpectedly**

Hence, you have two options to download the software for the project:

- **Pay Option**: Download and pay for the **expensive** software from the certified source with no security risks
- **Free Option**: Download the software for **free** from this uncertified source with the security risks indicated above

2.2 Medium Base Size

SCENARIO:

You are looking into downloading Alpha, an **expensive** software, that you need for a personal project.

Due to the cost of Alpha software, you searched online and found an uncertified source providing a download of Alpha software for **free** with the following security risks:

> Among **1,000** people who downloaded the software:
> **100** people's computers were **infected with viruses and crashed unexpectedly**

Hence, you have two options to download the software for the project:

- **Pay Option**: Download and pay for the **expensive** software from the certified source with no security risks
- **Free Option**: Download the software for **free** from this uncertified source with the security risks indicated above

2.3 Large Base Size

SCENARIO:

You are looking into downloading Zeta, an **expensive** software, that you need for a personal project.

Due to the cost of Zeta software, you searched online and found an uncertified source providing a download of Zeta software for **free** with the following security risks:

> Among **100,000** people who downloaded the software:
> **10,000** people's computers were **infected with viruses and crashed unexpectedly**

Hence, you have two options to download the software for the project:

- **Pay Option**: Download and pay for the **expensive** software from the certified source with no security risks
- **Free Option**: Download the software for **free** from this uncertified source with the security risks indicated above

APPENDIX C.

QUESTIONNAIRE

	Measurement Items
Perceived Risk	(PR1) Please indicate how risky you perceive the action of downloading this software for free from the uncertified source.
	(PR2) Please indicate the level of risk of downloading this software for free from the uncertified source.
	(PR3) Please rate the riskiness of downloading this software for free from the uncertified source.
Download Intention	(DI1) I intend to download this software for free from the uncertified source.
	(DI2) I plan to download this software for free from the uncertified source.
	(DI3) It is likely that I will download this software for free from the uncertified source.
Download Decision	What is your choice of downloading this software? • Option 1: Download and pay for the expensive software from the certified source with no security risks • Option 2: Download the software for free from this uncertified source with the security risks indicated above
General Information Security Awareness	(GISA1) Overall, I am aware of potential security threats and their negative consequences.
	(GISA2) I have sufficient knowledge about the effect of potential security problems. (Revised from original)
	(GISA3) I understand the concerns regarding the risks posed by information security.
Self-Efficacy	(SE1) I am confident that I can remove viruses from my computer.
	(SE2) I am confident that I can prevent unauthorized intrusion into my computer.
	(SE3) I believe I can configure my computer to protect it from viruses.
Cybersecurity Awareness	(CA1) I follow news and developments about virus technology.
	(CA2) I follow news and developments about anti-virus technology. (Revised from original)
	(CA3) I discuss Internet security issues with friends and people around me.
	(CA4) I read about the problems of malicious software intruding into Internet users' computers.
	(CA5) I seek advice from various sources on anti-virus products. (Revised from original)
	(CA6) I am aware of spyware problems and consequences.
Internet Structural Assurance	(ISA1) The Internet has enough safeguards to make me feel comfortable using it for online transactions.
	(ISA2) I feel assured that legal structures adequately protect me from problems on the Internet. (Revised from original)
	(ISA3) I feel assured that technological structures adequately protect

	me from problems on the Internet. (Revised from original)
	(ISA4) I feel confident that technological advances on the Internet make it safe for me to carry out online transactions.
	(ISA5) In general, the Internet is a safe environment to carry out online transactions.
General Risk-Taking Tendencies	(GRT1) Safety first. (Reverse coded)
	(GRT2) I prefer to avoid risks. (Reverse coded)
	(GRT3) I take risks regularly.
	(GRT4) I really dislike not knowing what is going to happen. (Reverse coded)
	(GRT5) I enjoy taking risks. (Revised from original)
	(GRT6) In general, I view myself as a ... (Risk avoider = 1 to Risk Seeker = 7)
Computer Security Risk-Taking Tendencies	(CSRT1) I do not take risks with computer security. (Reverse coded)
	(CSRT2) I generally avoid computer security risks. (Reverse coded)
	(CSRT3) I play it safe with computer security risks. (Reverse coded)
	(CSRT4) I prefer to avoid computer security risks. (Reverse coded)
	(CSRT5) I am not afraid of taking computer security risks.
	(CSRT6) I am willing to take risks with computer security.
	(CSRT7) With regard to computer security, I view myself as a ... (Risk avoider = 1 to Risk Seeker = 7)
Framing Manipulation Check	In the previous scenarios, what kind of information was provided? (Please check ALL that apply) • Option 1: Number of people's computers that were safe and secure • Option 2: Number of people's computers that were infected with viruses and crashed unexpectedly

APPENDIX D.

QUESTIONNAIRE OF DEMOGRAPHICS INFORMATION

1. What is your gender? (Male, Female, Other)
2. How old are you? (18-24, 25-34, 35-44, 45-54, 55-64, 65-74, 75-84, and 85 or older)
3. Please specify your ethnicity. (White, Black or African American, American Indian or Alaska Native, Asian, Native Hawaiian or Pacific Islander, Other, and Prefer Not to Disclose)
4. What is your marital status? (Married, Widowed, Divorced, Separated, and Never Married)
5. What is the highest level of school you have completed or the highest degree you have received? (Less than high school degree, High school graduate (high school diploma or equivalent including GED), Some college but no degree, Associate degree in college (2-year), Bachelor's degree in college (4-year), Master's degree, Doctoral degree, and Professional degree (JD, MD))
6. With regard to your education, what is your major area of study? (Please Specify)
7. Which of the following best describes your current employment status? (Employed full time, Employed part time, Unemployed looking for work, Unemployed not looking for work, Retired, and Student)
8. Please indicate your occupation: (Management, professional, and related; Sales and office; Farming, fishing, and forestry; Government; Retired; Unemployed and Other (Please Specify))
9. Which of the following best represents your annual personal income (before taxes) in the previous year? (Less than $10,000, $10,000 to $29,999, $30,000 to $49,999, $50,000 to $69,999, $70,000 to $89,999, $90,000 to $109,999, $110,000 to $129,999, $130,000 to $149,999, $150,000 or more, and Prefer not to disclose)

10. Which of the following best represents your annual household income (before taxes) in the previous year? (Less than $10,000, $10,000 to $49,999, $50,000 to $99,999, $100,000 to $149,999, $150,000 or $199,999, $200,000 to 249,999, More than $250,000, and Prefer not to disclose)
11. How much disposable income or allowance (i.e., the money you can spend as you want and not the money you spend on taxes, food, shelter and other basic needs) do you have per month? (Less than $100, $100 - $500, $501 - $1000, $1001 - $2000, More than $2000)
12. Approximately how many hours do you spend online per week? (1-5, 6-10, 11-15, 16-20, 20+)
13. How frequently do you download software from unknown sources? (Never, Sometimes, About half the time, Most of the time, and Always)

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.

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

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behaviour.

Akhawe, D., & Felt, A. P. (2013, August). Alice in Warningland: a large-scale field study of browser security warning effectiveness. In USENIX Security Symposium (Vol. 13).

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.

Beebe, N. L., Young, D. K., & Chang, F. (2014). Framing Information Security Budget Requests to Influence Investment Decisions. CAIS, 35, 7.

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 quarterly, 34(3), 523-548.

Chaiken, S., & Eagly, A. H. (1989). Heuristic and systematic information processing within and. Unintended thought, 212, 212-252.

Chen, J., Gates, C. S., Li, N., & Proctor, R. W. (2015). Influence of risk/safety information framing on android app-installation decisions. Journal of Cognitive Engineering and Decision Making, 9(2), 149-168.

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

Darwish, A., & Bataineh, E. (2012, December). Eye tracking analysis of browser security indicators. In Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on (pp. 1-6). IEEE.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly, 319-340.

Davis, M. A., & Bobko, P. (1986). Contextual effects on escalation processes in public sector decision making. Organizational Behavior and Human Decision Processes, 37(1), 121-138.

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

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. Journal of the Association for Information Systems, 8(7), 23.

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

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

Felt, A. P., Ainslie, A., Reeder, R. W., Consolvo, S., Thyagaraja, S., Bettes, A., ... & Grimes, J. (2015, April). Improving SSL warnings: comprehension and adherence. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 2893-2902). ACM.

Field, A. (2009). Discopering statistics using SPSS, Thrid Edition.

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

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: An introduction to theory and research.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? internet security and human vulnerability. Journal of the Association for Information Systems, 18(1), 22.

Greenhouse, S. W., & Geisser, S. (1959). On methods in the analysis of profile data. Psychometrika, 24(2), 95-112.

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

Helander, M. G., & Du, X. (1999). From Kano To Kahneman. A comparison of models to predict customer needs. In Proceedings of the Conference on TQM and Human Factors (pp. 322-329).

Huynh, H., & Feldt, L. S. (1976). Estimation of the Box correction for degrees of freedom from sample data in randomized block and split-plot designs. Journal of Educational Statistics, 1(1), 69-82.

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

Jeong, S. W., Fiore, A. M., Niehm, L. S., & Lorenz, F. O. (2009). The role of experiential value in online shopping: The impacts of product presentation on consumer responses towards an apparel web site. Internet Research, 19(1), 105-124.

Kahneman, D., & Tversky, A. (1979). Prospect theory: an analysis of decision under risk. Econometrica, 47(2), 263-292.

Larrick, R. P., Smith, E. E., & Yates, J. F. (1992, November). Reflecting on the reflection effect: disrupting the effects of framing through thought. In Meetings of the Society of Judgment and Decision Making, November, St. Louis, MO.

Levin, I. P., & Chapman, D. (1990). Risk taking, frame of reference, and characterization of victim groups in AIDS treatment decisions. Journal of Experimental Social Psychology, 26(5), 421-434.

Levin, I. P., Schneider, S. L., & Gaeth, G. J. (1998). All frames are not created equal: a typology and critical analysis of framing effects. Organizational Behavior and Human Decision Processes, 76(2), 149-188.

Mauchly, J. W. (1940). Significance test for sphericity of a normal n-variate distribution. The Annals of Mathematical Statistics, 11(2), 204-209.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information systems research, 13(3), 334-359.

Meertens, R. M., & Lion, R. (2008). Measuring an individual's tendency to take risks: the risk propensity scale 1. Journal of Applied Social Psychology, 38(6), 1506-1520.

Mongin, P. (1997). Expected utility theory. Handbook of economic methodology, 342350.

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

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.

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

Rosoff, H., Cui, J., & John, R. S. (2013). Heuristics and biases in cyber security dilemmas. Environment Systems and Decisions, 33(4), 517-529.

Schroeder, N. J., Grimaila, M. R., & Schroeder, N. (2006, May). Revealing prospect theory bias in information security decision making. In Emerging Trends and Challenges in Information Technology Management: 2006 Information Resources Management Association International Conference (pp. 176-179).

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

Smith, S. N., Nah, F. F. H., & Cheng, M. X. (2016, July). The impact of security cues on user perceived security in e-commerce. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 164-173). Springer, Cham.

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.

Takemura, K. (1994). Influence of elaboration on the framing of decision. The Journal of Psychology, 128(1), 33-39.

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

Valecha, R., Chen, R., Herath, T., Vishwanath, A., Wang, J. R., & Rao, H. R. (2016). Reward-based and risk-based persuasion in phishing emails. In Proceedings of the 2016 Dewald Roode Workshop on Information Systems Security Research, IFIP WG8 (Vol. 11, pp. 1-18).

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

Wang, X. T. (1996a). Domain-specific rationality in human choices: Violations of utility axioms and social contexts. Cognition, 60, 31-63.

Wang, X. T., & Johnston, V. S. (1995). Perceived social context and risk preference: A re-examination of framing effects in a life–death decision problem. Journal of Behavioral Decision Making, 8, 279-293.

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

Woodworth, R. S. (1918). Dynamic psychology. Columbia University Press.

VITA

Xinhui Zhan was born in Yinchuan, Ningxia, China. She received her Bachelor's degree in Communication Engineering from Communication University of China in June, 2013. She received her Master of Fine Arts in Media Production from State University of New York at Buffalo in June, 2016.

She joined Missouri University of Science and Technology (formerly known as University of Missouri – Rolla) in Fall 2017. In May 2019, she received her M.S. in Information Science and Technology from Missouri University of Science and Technology.