Presentation of Computer Security Risks:

Impact of Framing and Base Size

Xinhui Zhan, Fiona Fui-Hoon Nah, Keng Siau, Richard H. Hall
Missouri University of Science and Technology
xzxpd@mst.edu, nahf@mst.edu, siauk@mst.edu, rhall@mst.edu

Maggie Cheng
Illinois Institute of Technology
maggie.cheng@iit.edu

Abstract

This research explores how the presentation of computer security risks impacts users' risk perceptions and behavior. It draws on Prospect Theory to generate hypotheses related to users' decision-making in the computer security context. A 2 × 3 mixed factorial experimental design (N = 178) was carried out and the results show that framing and base size of information on computer security risks influence 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. The findings from this research suggest that using negative framing and large base size to communicate computer security risks is an effective strategy to lower risk-taking behavior of users.

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

Acknowledgement: We acknowledge National Science Foundation EAGER funding (CNS/1537538) for the support of this research.

1. Introduction

The occurrence of computer security threats is common on the Internet. Users play a fundamental role in the identification and prevention of computer threats (Stanton et al., 2004) as they are expected to assess cybersecurity threats before carrying out an action online such as conducting an online transaction, accessing a URL, and downloading a file. According to a report by IBM, 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, users sometimes fail to detect computer security threats. For example, when users make decisions related to downloading software from anonymous sources or providing personal information to conduct online transactions, their choices could bring negative outcomes, such as data and information leakage or damage to their personal computer. Thus, it is crucial to issue warnings or information associated with computer security risks.

The literature suggests that providing more effective security warning systems can reduce computer security risks and protect users' private information (Darwish & Bataineh, 2012; Smith et al., 2016). Hence, users' assessments and perceptions of the messages in computer security warnings can have an impact on their behavior. Thus, research to examine the presentation of information security messages and how they affect users' risk perceptions play a crucial role in predicting and understanding users' behavior in computer security.

The goal of this research is to explore the presentation of information on computer security risks and their effects on users' risk-taking behavior. A laboratory experiment was conducted to examine the impact of framing computer security risk information and varying base sizes of the information on users' risk perceptions and behavior. Specifically, we are interested in studying whether negatively framed messages give rise to risk-averse actions as compared to positively framed messages and whether increasing the base size of evidence on computer security threats decreases users' risk-taking behavior.

The rest of this paper is organized as follows. Section 2 presents a review of related literature. Section 3 presents the theoretical foundation, and Section 4 shows the hypotheses. Section 5 describes the research methodology, design, and procedure. Section 6 and Section 7 present and discuss the findings. Section 8 concludes the paper.

2. Review of Literature

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.

Understanding human decision-making process is key to explaining users' behavior when faced with cybersecurity threats. Several studies have focused on developing better interface and

warnings 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 warning (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 be provided to convey recommended actions to users even though they may pose an interruption to 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).

Smith, Nah, and Cheng (2016) examined user assessment of security in e-commerce by varying cues/miscues (i.e., HTTP vs. HTTPS, fraudulent vs. authentic URL, padlocks beside vs. within fields) presented on web pages. They conducted a within-subjects experiment where users rated the perceived security, trustworthiness, and safety of 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.

According to Prospect theory, 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 show 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, the framing effect tended to be reduced when they were required to explain their choices (Larrick et al., 1992). The framing effect could also be eliminated if users are encouraged to think through the rationale underlying their choices (Takemura, 1994). Moreover, if users are experts in a particular area, the framing effect would also be reduced (Davis and Bobko, 1986).

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 the contexts of 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 indicate that subjects exhibited no difference in their choice between safe versus risky decision options regardless of whether the outcomes were framed as gains or losses.

Cybersecurity researchers also expanded their 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 be attractive to users by offering a reward or benefit, such as an email that informs the recipient about winning a lottery. On the other hand, risk-based persuasion is designed to scare people by highlighting a potential risk. Their 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 their 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 increase users' app-installation decisions.

3. Theoretical Foundation: Prospect Theory

Prospect theory 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 decision choices based on the framing of the options given to them. They also explored how framing can affect choices in a hypothetical life and death situation, 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
B. 1/3 probability of saving 600 people and 2/3 probability of saving none

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

C. 400 people will die
D. 1/3 probability that none will die and 2/3 probability that 600 will die

Option A and option B in positive framing are mathematically equivalent to Option C and Option D in negative framing since they provide the same utility (satisfaction). "200 people will

be saved" implies that among 600 people, 200 of them will be saved, which is equivalent to "400 people will die" in negative framing. Similarly, "1/3 probability of saving 600 people and 2/3 probability of saving none" is equivalent to "1/3 probability that none will die and 2/3 probability that 600 will die". Given their equivalence, subjects should choose their decision option in a similar way in either framing.

Surprisingly, in the positively framed scenario, 72% of the subjects selected the certainty option (i.e., option A) and 28% selected the risky option (i.e., option B). On the contrary, in the negatively framed scenario, only 22% of the subjects selected the certainty outcome (i.e., option C) and 78% selected the risky option (i.e., option D). 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 other option due to the fear of losing 400 people's lives due to the negative framing. That is to say, people have the tendency to avoid losses and go for sure wins.

Two factors have been used to explain the framing effect: the reference point, and the value function. The reference point refers to the status quo, which determines 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 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 1). The gain side is concave which suggests that people are risk-averse when making 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.

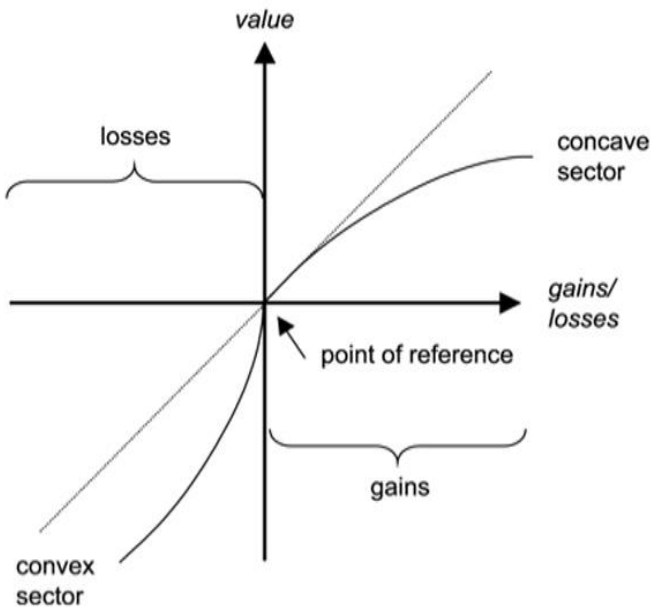

Figure 1. Value Function

In the "Asian disease" problem, the positive framing refers to saving lives, so the status quo is "zero people saved", thus both options A and B are viewed as gains. In the negatively framed problem, both options C and D refer to death. The reference point, in this case, is "zero people died" and the two options are viewed as losses. Drawing on the value function, the outcomes 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.

4. Hypothesis Development and Research Model

Prospect theory purports that individuals weigh losses more heavily than gains. We extend the term "gains" and "losses" to two different and opposite ways of framing information – positive and negative framing. Specifically, when a situation is framed negatively, the negative consequence or attribute is emphasized. On the other hand, when a situation is positively framed, the positive aspects are more salient. For example, a piece of meat can be presented as "75% fat-free" or "25% fat".

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). We hypothesize that the framing of the consequences of decision choices affects users' perceived risk such that negative framing is perceived to be of greater magnitude or impact than

positive framing because losses exert a stronger influence over people's perceptions than gains. Hence, we propose the following hypothesis:

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". Larger samples usually provide more reliable information (Bernoulli, 1713). In other words, "1 out of 100" might be considered a contingency whereas the latter (i.e., "100 out of 10000") represents a more reliable probability. In other words, people are more confident in their decision when the information was provided with a larger base size (Nisbett et al., 1983). Wang and Johnston (1995) further extended the "Asian Disease Problem" study by varying the number of people in the base size (i.e., 6, 60, 600 and 6000) in both gain and loss conditions. Their results reveal 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 larger 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 sizes were 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 salient 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, the effect of framing on risk perception also increases.

Technology Acceptance Model (TAM) is a well-known and well-established information systems theory that models users' acceptance of information technology (Davis, 1989). 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. In the computer security context, users' attitude toward downloading a software that poses some security risks will thus influence their download intention, and a key variable that influences users' attitude is their perception of the risks involved in the download. Hence, we hypothesize that the higher the perceived risk, the lower the behavioral download intention.

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

According to TAM, download intention is an antecedent of the behavior to download the software. In other words, the higher the intention to engage in the download behavior, the more likely the user will make the decision to perform the download action. Hence, we hypothesize that download intention is positively associated with download decision.

H5: Download intention is positively associated with download decision.

Drawing on Prospect Theory and TAM, five hypotheses have been generated and the research model is shown in Figure 2. 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.

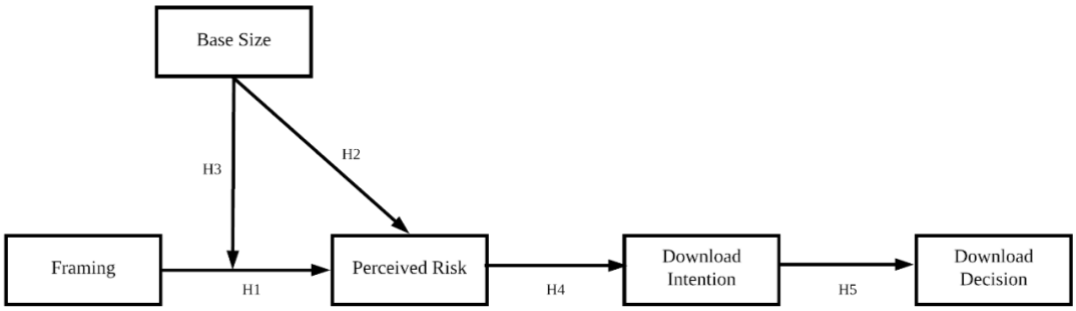

Figure 2. Research Model

5. Research Methodology

We conducted a 2 (positive/negative framing) × 3 (small, medium and large base size) mixed factorial experimental design to test the hypotheses and assess the relationship of framing and base size of computer security risk information on users' behavior. A scenario-based survey was used to manipulate the independent variables (i.e., framing and base size) in the experimental design as well as measure the rest of the variables in the research model. Research subjects were

recruited through the crowdsourcing website, Amazon Mechanical Turk (MTurk). Our respondents are at least 18 years of age and they reside in the United State.

5.1 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.

Framing was first studied based on the Asian disease problem, also referred to as "framing of options". Later on, researchers discussed and explored other types of framing manipulations, including 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 that includes 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 (i.e., positive framing) or 1 out of 10 people's computers were infected with viruses (i.e., negative framing). In this study, framing is a between-subjects variable where subjects were randomly assigned to one of the two framing conditions.

Base size was operationalized as 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. For example, a download with 10% virus infection rate could be presented with different base sizes when framing positively: 9 out of 10 people's computers were secure vs. 900 out of 1000 people's computers were secure. Moreover, in order to mask the systematic patterns of the base size manipulations from the subjects, two analogous scenarios (with 5% and 20% computer virus infection rates) were inserted as distractors.

The five scenarios (three main scenarios and two distractors) were presented in a randomized order to counter-balance any potential ordering effect. The three main scenarios for each of positive and negative framing conditions are presented in the Appendix. Table 1 presents the operationalization of the independent variables, framing and base size.

Table 1. Operationalization of Framing and Base Size

Framing / Base Size	Positive	Negative
Small: 10	Among **10** people who downloaded the software: **9** people's computers were safe and secure	Among **10** people who downloaded the software: **1** person's computer was infected with viruses and crashed unexpectedly
Medium: 1,000	Among **1,000** people who downloaded the software: **900** people's computers were safe and secure	Among **1,000** people who downloaded the software: **100** people's computers were infected with viruses and crashed unexpectedly
Large: 100,000	Among **100,000** people who downloaded the software: **90,000** people's computers were safe and secure	Among **100,000** people who downloaded the software: **10,000** people's computers were infected with viruses and crashed unexpectedly

5.2 Dependent Variables and Covariates

After the subject completed each scenario, a short questionnaire was used to assess the perceived risk, download intention, and download decision (see Table 2 for the items). A three-item scale was used to assess perceived risk. The first item was adopted from Weber et al. (2002) and the two other items were self-developed. These three items used the 5-point Likert scale (not at all risky/no risk at all = 1 to extremely risky/extremely high risk = 5). Subjects were also asked to rate their intention to download the software. The measurement items for intention were adopted from Ajzen's (1991) and the 7-point Likert scale (strongly disagree = 1 to strongly agree = 7) was used for the three items. After assessing download intention and perceived risk, subjects were asked to answer a question about their download decision.

After subjects completed all five scenarios, they also responded to a post-experimental questionnaire that captured the following demographic information and covariates:

- 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.

A manipulation check question for framing was also included in the questionnaire.

Table 2. Measurement of Dependent Variables

	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

5.3 Experimental Task

As mentioned earlier, the subjects were asked to assess five software download scenarios of which three of them were the experimental stimuli and two of them were distractors. The software application in each of the three "within-subjects" scenarios was associated with a fixed percentage level of computer security risk, i.e., 10% of those who downloaded the software had their computers infected with viruses, but differ in their base sizes (i.e., number of people who had downloaded the software) of the computer security risk.

We detailed each scenario as a free download of an expensive software from an uncertified source:

> *"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."*

Subjects were presented with the five "within-subjects" scenarios that they have to respond to, as explained earlier.

6. Findings

A total of 205 people based in the US participated in the study by filling out the questionnaire in Amazon Mechanical Turk. The number of usable responses is 178 after removing data points that failed the attendance check questions. We used the SPSS software to analyze the data collected. The analysis included the assessment of 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.

Table 3 shows the Cronbach's alpha coefficients. Cronbach's alpha coefficients of at least 0.7 indicate good reliability of the constructs (Nunnally et al., 1967). Since all of the Cronbach's alpha coefficients (see Table 3) are above 0.9, the measurement shows very high reliability.

Table 3. Results of Reliability Analysis

Variable	Cronbach's Alpha Coefficient
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

6.1 Repeated Measures ANOVA

Repeated measures ANOVA was used to assess overall differences between related means or the mean scores of two or more within-subjects conditions. Given that we have 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.

Table 4 shows the descriptive statistics for the effect of Positive and Negative Framing on Perceived Risk. Framing has a significant main effect on Perceived Risk ($p < 0.001$). Subjects who experienced Negative Framing (Mean = 3.83, SD = 1.02) exhibited greater Perceived Risk than those who experienced Positive Framing (Mean = 3.10, SD = 1.08). Hence, H1 is supported.

Table 4. Descriptive Statistics of Between-Subjects Effect of Framing on Perceived Risk

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

Table 5 provides the descriptive statistics and the means for Perceived Risk at the different levels of Base Size and Framing.

Table 5. Descriptive Statistics for Perceived Risk

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

Table 6 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. The mean scores for Perceived Risk are statistically different ($p < 0.001$) across the three levels of Base Size. The perceived risk in the large base size condition (Mean = 3.64, SD = 1.09) is larger than that in the medium base size condition (Mean = 3.45, SD = 1.07), and the perceived risk in the medium base size condition is larger than that in the small base size condition (Mean = 3.31, SD = 1.15). Since the overall ANOVA result for the three levels of Base Size is significant, we also ran the post-hoc tests to see which levels of the Base Size are different. According to the post-hoc tests presented in Table 7, there is a significant effect across every level of Base Size on Perceived Risk. Hence, there is a significant difference in Perceived Risk between small and medium Base Size ($p = 0.01 < 0.05$, MD = 0.14) and between medium and large Base Size ($p < 0.001$, MD = 0.19). As the Base Size increases, Perceived Risk is also significantly increased. Hence, H2 is supported.

Table 6. 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	0.000
	Greenhouse-Geisser	9.73	1.76	5.53	17.07	0.000
	Huynh-Feldt	9.73	1.79	5.44	17.07	0.000
	Lower-bound	9.73	1.00	9.73	17.07	0.000
Framing * Base Size	Sphericity Assumed	0.04	2.00	0.02	0.07	0.930
	Greenhouse-Geisser	0.04	1.76	0.02	0.07	0.909
	Huynh-Feldt	0.04	1.79	0.02	0.07	0.912
	Lower-bound	0.04	1.00	0.04	0.07	0.787
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		

Table 7. 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	0.005	-0.24	-0.04
Medium	**Large**	-0.19	0.05	0.000	-0.29	-0.09

Framing*Base Size. According to the results of repeated measures ANOVA presented in Table 6, there is no interaction effect between Framing and Base Size on Perceived Risk ($p = 0.909 > 0.05$). Hence, H3 is not supported. The relationship between framing and base size is shown in Figure 3, where no interaction effect is observed.

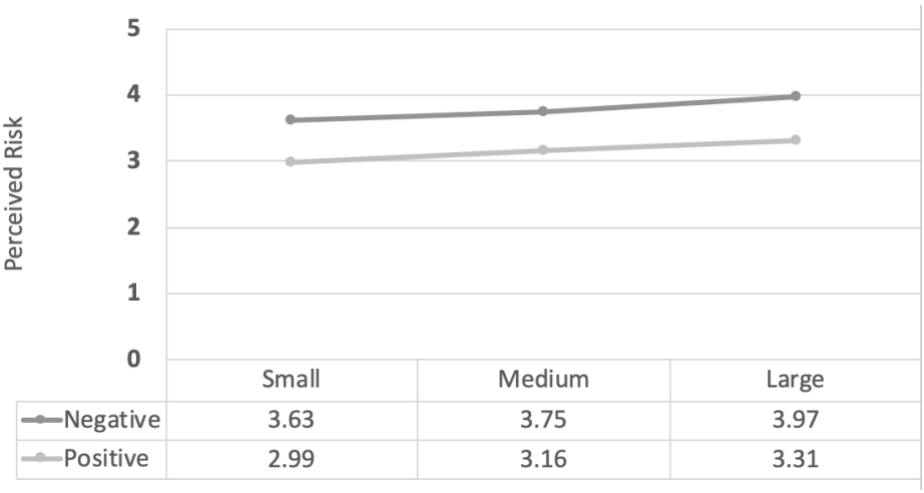

Figure 3. Effects of Framing and Base Size on Perceived Risk

6.2 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. Given the nested nature of the data, we conducted mixed model regression analysis to test H4 and H5. The result of mixed model regression analysis for download intention is shown in Table 8, where the effect of Perceived Risk on Download Intention is significant ($p < 0.001$). Hence, H4 is supported.

Table 8. Test of the Effect of Perceived Risk on Download Intention

Source	Numerator df	Denominator df	F	Sig.
Intercept	1	463.72	363.30	<0.001
Perceived Risk	12	403.64	25.64	<0.001

The result of mixed model regression analysis for download decision is presented in Table 9. As shown in Table 9, the effect of Download Intention on Download Decision is significant ($p < 0.001$). Download intentions are positively associated with download decisions. Hence, H5 is also supported.

Table 9. Test of the Effect of Download Intention on Download Decision

Source	Numerator df	Denominator df	F	Sig.
Intercept	1	411.36	3612.96	<0.001
Download Intention	18	436.36	62.32	<0.001

Table 10 summarizes the results of hypothesis testing. In summary, H1, H2, H4, and H5 are supported and H3 is not supported.

Table 10. 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

7. Discussions of Findings

The results of our study suggest that framing of security related information influences users' perceptions of risks. In addition, the results demonstrate that base size, manipulated through displaying the total number of people who had downloaded the software with potential security threats, influences users' perceived risks. However, the results do not show any interaction effect of base size and framing on users' behavior, which is inconsistent with the findings by Wang and Johnston (1995). Hence, based on our study, base size does not moderate the effect of framing on perceived risk. Our 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 perceived at a greater magnitude than a gain. Our finding is in line with Prospect Theory and suggests that users' perceived computer security risk is higher in negative framing than positive framing.

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 reliability associated with the 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, presenting negatively framed computer security risks is an effective way to reduce or minimize computer security risk-taking behavior. In other words, 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.

8. Conclusions and Implications

This research examines the impact of presenting positively and negatively framed computer security risk information that varied in base sizes on the computer security behavior and risk perceptions of users. We also examined the relationships between risk perceptions and download intentions, as well as download intentions and download decisions.

Our findings have theoretical and practical implications. We assessed the Prospect Theory in a computer security context to understand whether negatively framed cybersecurity risk information could lead users to engage in less risk-taking behavior as compared to positively framed risk information. The findings support the Prospect Theory and suggest that the framing of computer security 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. Hence, negative framing is indeed the recommended way to present computer security risks to users. In addition, our study also assessed the base size effect (Wang and Johnston, 1995; Levin and Chapman, 1990), which supports the idea that people tend to be less risk seeking as the base size of computer risk information increases. Our study confirms that the base size effect was found in both positive and negative framing. Hence, when the base size of computer risk information is large, it is recommended that the base size be presented as part of the information on computer security risks. Information on base size affects people's risk perceptions such that the greater the base size, the higher the perceived risk.

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.

References

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

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).

Bernoulli, J. (1713). Ars conjectandi. Basel: Thurnisius. Edith Sylla's English translation, The Art of Conjecturing, together with Letter to a Friend on Sets in Court Tennis. Johns Hopkins University Press (Oscar Sheynin's English translation of Part IV, dated 2005, is at www.sheynin.de)

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.

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.

Darwish, A., & Bataineh, E. (2012, December). Eye tracking analysis of browser security indicators. In Proceedings of the International Conference on Computer Systems and Industrial Informatics (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.

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.

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.

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

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.

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.

Nisbett, R. E., Krantz, D. H., Jepson, C., & Kunda, Z. (1983). The use of statistical heuristics in everyday inductive reasoning. Psychological Review, 90, 339–363.

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

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

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).

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.

APPENDIX:

EXPERIMENTAL CONDITIONS

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

---

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