Summer 2018

Impact of probable and guaranteed monetary value on cybersecurity behavior of users

Santhosh Kumar Ravindran

Department:

IMPACT OF PROBABLE AND GUARANTEED MONETARY VALUE ON CYBERSECURITY BEHAVIOR OF USERS

by

SANTHOSH KUMAR RAVINDRAN

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

2018

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

ABSTRACT

This research examines the impact of probable and guaranteed monetary gains and losses on users' cybersecurity behavior. It also examines perceptual outcomes such as threat severity, trust, and fear that are associated with users' cybersecurity behavior. Drawing on Prospect Theory in the behavioral economics and decision-making literature, hypotheses were generated for the research. The hypotheses state that: (i) users are more willing to engage in risky computer security behavior to avoid a loss than to receive a gain, (ii) users exhibit a higher tipping point of expected monetary value to receive a gain than to avoid a loss for engaging in risky computer security behavior, (iii) users are more willing to engage in risky computer security behavior to avoid a guaranteed loss than a probable loss, controlling for the amount of expected loss, (iv) users are more willing to engage in risky computer security behavior to receive a guaranteed gain than a probable gain, controlling for the amount of expected gain, and (v) users exhibit a higher tipping point of expected monetary value to engage in risky computer security behavior when presented with a probable gain (or loss) as compared to a guaranteed gain (or loss). A 2 x 2 between-subjects experimental design was used to test the hypotheses. The findings indicate that there is no difference in users' risky computer security behavior between receiving a gain and avoiding a loss. However, users exhibit a higher tipping point of expected monetary value for probable gains and losses than guaranteed gains and losses.

Keywords: Cybersecurity, Prospect Theory, Gain, Loss, Monetary Value.

ACKNOWLEDGMENTS

I would like to express my gratitude to my advisor, Dr. Fiona Fui-Hoon Nah, for the endless support, guidance, and encouragement. Her patience, knowledge, and vast experience in research has been exceptional. She helped me from the start till the end of this research and provided me with all the guidance and help required to complete my research as well as assisted me with data analysis. It has been a great learning experience under her guidance.

I would like to express my gratitude to the rest of my thesis committee members, Dr. Keng Siau and Dr. Richard Hall, for their support, feedback, and suggestions that helped me to further improve and enhance this research.

I would like to thank Dr. Barry Flachsbart. Ms. Yu-Hsien Chiu, Dr. Steve Liu, Dr. Chevy Fang, Dr. Sarah Stanley, Dr. Nathan Twyman, Dr. Richard Hall, Dr. Hongxian Zhang, Dr. Keng Siau, and Dr. Carla Bates for allowing me to recruit subjects for the experiment in their classes. I would also like to acknowledge the Psychology department for offering subjects for the experiment.

I would like to express my gratitude to all the Laboratory of Information Technology and Evaluation (LITE) students, especially to Cooper Broman, Alec Mcdaniel, Kyle Johnson, Luis Emmanuel Ocampo, Bryan Fox, and Andrew Hackett, for pilot testing the experimental study and in helping me to set up lab sessions for conducting the experimental study. I also thank National Science Foundation for the research funding.

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

TABLE OF CONTENTS

Page

LIST OF ILLUSTRATIONS

Page

LIST OF TABLES

Page

1. INTRODUCTION

The architecture of information security in an organization is dependent on the users, technology, and cybersecurity policies. Users play a significant role as they interact with the different components of an organization's information security architecture. A study by Sasse et al. (2001) indicates that users are a main cause of intrusions to the cybersecurity infrastructure in organizations. They found that the actions of users toward cybersecurity threats act as major causes of malicious intrusions and cybersecurity attacks. Users are advised to follow standard information security policies framed by the information security division of their organization, even though many do not, and instead, they based their actions on personal judgements. Chan and Mubarak (2012) state that the lack of cybersecurity knowledge is one of the main causes for cybersecurity threats in organizations. Major cybersecurity vulnerabilities in organizations are mainly caused by the lack of awareness about information security policies which can lead to attacks such as phishing, malware, mal-advertising, and drive-by downloads.

Spontaneous actions or misjudgments of users in cybersecurity related scenarios, such as those related to phishing emails or mal-advertisements, could pose a huge threat to an organization's security infrastructure. Chan and Mubarak (2012) found that despite maintaining a highly secure infrastructure, the lack of security awareness about security threats and attacks was the main reason for organizational vulnerability to cybersecurity threats. For example: Users' lack of awareness of phishing attacks or threats associated with downloading software from untrusted developers could lead to loss of enterprise data or data breaches in their organization. Although security awareness can be increased by

organizing training sessions and by explaining the information security policy to users, improving security awareness alone does not guarantee that the rules in the organization's cybersecurity policy will be followed.

The literature indicates that users are the most vulnerable elements in the cybersecurity infrastructure of an organization (Siponen, 2000a). Phishing attacks have been the most common information security threat to organizations and have been the most challenging attack to evade despite providing training to users. Most of the phishing attacks that are targeted at users contain a persuasive message to either receive a benefit (e.g., monetary gain) or overcome a threat (e.g., monetary loss). These messages persuade users to take a risky cybersecurity action by downloading an uncertified software or visiting a malicious website to avoid a loss or receive a benefit or gain. Such scenarios, which are common online threats, warrant the need for further research to understand the impact of monetary gains and losses on users' cybersecurity risk taking behavior. For this thesis, we conducted an experiment to assess the effect of probable and guaranteed monetary gains and losses on users' behavior in the context of cybersecurity.

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 provides the data analysis for the research. Section 6 discusses the results. Section 7 provides the limitations and directions for future research. Section 8 provides the conclusion for the thesis.

2. LITERATURE REVIEW

Chapter 2 provides a review of the literature on the effect of user behavior on information security as well as on message framing in the context of information security.

2.1. EFFECT OF USER BEHAVIOR ON INFORMATION SECURITY

Various processes for managing cybersecurity, such as the standardized framework for implementing security policies, exist in organizations. In this section, past empirical studies that are related to factors influencing user behavior in the context of cybersecurity will be reviewed. Siponen (2000a) states that users are the most vulnerable targets of cybersecurity threats in an organization. His study indicates that end users in organizations do not follow security guidelines, leading to cybersecurity threats such as phishing, malware, and other attacks.

Siponen (2000b) also stresses that even though the importance of the role of motivation in cybersecurity is largely understood, it is not practiced effectively in organizations. A review of the existing literature also indicates that risk perception is a factor influencing users' course of actions. In the computer security domain, Farahmand and Spafford (2013) state that individuals within an organization (i.e., insiders) may be deterred from undesirable computer security behaviors by reducing their motivation to misbehave and conveying that attempts to misbehave will present too much risk. As Vardi and Weitz (2004) noted in their research, the role of the employees is significant for the information security infrastructure of the organization, and it is very important for employees to adhere to the organizational policies to avoid security threats. Shoshitaishvili

et al. (2014) analyzed a team competition in cybersecurity challenges. Tasks were used to present different levels of risks to the teams, and it was found that teams were willing to engage in riskier tasks if those tasks provided higher rewards, measured in terms of competition points. In other words, the teams were willing to engage in riskier behavior when they perceived a higher level of reward because of their actions. A study which was based on Protection Motivation Theory (PMT) states that users' behavior in information security can be predicted using their self-efficacy (LaRose et al., 2008). Self-efficacy is defined as a belief that a user possesses towards achieving or accomplishing certain goals (LaRose et al., 2008). A survey-based research by Woon et al. (2005) indicates that perceived severity, response cost, perceived susceptibility and self-efficacy have an effect on cybersecurity behavior of users (Woon et al., 2005). Perceived severity refers to one's understanding of the severity of the consequences of an event. The authors found that users decide on their choice of action based on perceived severity and perceived vulnerability. Perceived vulnerability is defined as one's assessment of the probability of a threatening event and its effect on oneself. Response cost refers to perceived opportunity costs (which can be either money, time, or effort) that the user experiences due to adoption of the recommended behavior. The research study by Pahnila et al. (2007) on user behavior in cybersecurity considers various other factors that include sanctions, information quality and rewards to understand the possible effects of these factors on the cybersecurity behavior of users (Pahnila et al., 2007).

Maddux and Rogers (1983) have shown that coping response has a positive influence towards behavioral intents, which can result in implementation of the recommended compliance behavior. Coping response refers to the behavioral responses

or actions that people take to overcome stressful situations (Maddux and Rogers, 1983). Various studies in the literature have assessed the effect of fear appeal on cybersecurity behavior of users when they are in a high-risk environment. Johnston and Warkentin (2010) found that fear appeal could be used to persuade users to alter their cybersecurity behavior in order to avoid cybersecurity threats and risks. The behavior of users also depends on their self-efficacy and perceived threat vulnerability (Johnston & Warkentin, 2010).

In a review of the literature by Lebek et al. (2013), they summarized the reasons for users' security responses based on the most frequently applied theories in behavioral sciences: Theory of Reasoned Action (TRA) / Theory of Planned Behavior (TPB), General Deterrence Theory (GDT), Protection Motivation Theory (PMT), and Technology Acceptance Model (TAM). Aurigemma & Panko (2010) found that the intentions of a user to comply with information security policies (ISP) depends on his/her own evaluation and belief towards the process.

Aurigemma and Panko (2010) also found that the greater the notion of control the user develops over his or her actions, the greater is the intention to comply with the ISP of the organization. Based on GDT, the research in criminal justice by D'Arcy et al. (2009) indicates that the possible repercussions of a decision, such as perceived certainty of sanctions or the loss that a user might face, influences his/her decision on ISP compliance. In a study based on PMT by Bulgurcu et al. (2010), they found that a user's attitude towards the information security policies of an organization is often influenced by two factors, threat appraisal and coping appraisal, where the user analyzes the threats involved and adopts the technology to prevent cybersecurity threats.

Past literature also suggests that even though users possess prior knowledge about cybersecurity threats and the suitable recommended actions, in some cases, the users take risky cybersecurity actions for benefits or rewards (Lee & Kozar, 2005; Stanton et al., 2005; Sasse et al., 2001). The Table 2.1 provides the summary of existing literature on the effect of user behavior on information security.

Table 2.1. Summary of Literature Review on the Effect of User Behavior on Information Security

Reference	Description	Theory
Aurigemma & Panko (2010)	The authors found that users' intentions to comply with information security policies of the organization depends on his/her own evaluation and belief towards the process.	Not Applicable
Bulgurcu et al. (2010)	The authors found that users' attitude is affected by the cost associated with the consequences of his/her compliance/non-compliance behavior.	Protection Motivation Theory
D'Arcy et al. (2009)	The authors analyzed the possible repercussions of a decision such as the perceived uncertainty of sanctions or the loss that a user might face and its influence on his/her decision on the ISP compliance.	General Deterrence Theory

Table 2.1. Summary of Literature Review on the Effect of User Behavior on Information Security (cont.)

Reference	Description	Theory
Johnston & Warkentin (2010)	The authors proposed that fear appeals affect users' security behavioral intents, but the effect is not constant.	Fear Appeal Theory, and Protection Motivation Theory
LaRose et al. (2008)	The authors found that users' cybersecurity behavior mainly depends on social connections and self-efficacy.	Protection Motivation Theory and Social Cognitive Theory
Lebek et al. (2013)	The authors identified the reasons for users' security responses and summarized them using four main behavioral theories: General Deterrence Theory, Technology Acceptance Model, Theory of Planned Behavior, and Protection Motivation Theory.	Theory of Reasoned Action, Theory of Planned Behavior, Technology Acceptance Model, and General Deterrence Theory
Pahnila et al. (2007)	The authors found that attitude, normative beliefs, and habits influence ISP compliance intention, and threat appraisal and facilitating conditions influence attitude toward compliance.	General Deterrence Theory, Protection Motivation Theory
Shoshitaishvili et al. (2014)	The authors analyzed users' cybersecurity behavior through a competition in which teams competed in cybersecurity challenges. The study observed that the teams were willing to engage in riskier behavior when they perceived a higher level of reward because of their actions.	Not Applicable

Table 2.1. Summary of Literature Review on the Effect of User Behavior on Information Security (cont.)

Reference	Description	Theory
Siponen (2000a)	The author analyzed different methods to reduce user related faults in information systems security and examined the strengths and weaknesses of these methods.	Theory of Planned Behavior, Technology Acceptance Model, Theory of Reasoned Action, and General Deterrence Theory
Woon et al. (2005)	The authors found that users' choice of action was based on perceived severity and perceived vulnerability.	Protection Motivation Theory

2.2. MESSAGE FRAMING

The literature has also examined the effect of positively and negatively framed messages on users' behavior (Aaker & Lee, 2001; Shiv, Edell & Payne, 2004). Various studies have also been conducted to understand users' behavior and decision-making process based on Prospect Theory which states that the outcomes of an individual can be influenced by the way the message is framed (Tversky & Kahneman, 1986). Users generally select their choices by considering personal gains or losses conveyed in the message. Prospect theory states that users tend to perceive losses more than gains, which is also known as loss aversion (Tversky & Kahneman, 1984). Researchers explain loss aversion as a behavior observed in people, where people try to avoid a loss in scenarios where there is a risk involved (Tversky & Kahneman, 1984). The effect of message framing across various decision-making perspectives has been studied from financial and socio psychological standpoints, based on funds and social predicaments in a research

study by Brewer and Kramer (1986). Similarly, in the cybersecurity domain, researchers have studied the impact of message framing on reliant variables covering threat awareness, as stated in a research study by Lee and Aaker (2004). Message framing also includes highlighting the advantages and the constructive aspects of selecting a choice or the disadvantages of not selecting a choice (Aaker & Lee, 2001). Protection Motivation Theory (PMT) based research studies related to health have been conducted to understand what type of promotional messages would persuade a user, thereby preventing the user from taking an action when confronted with a risk. Pechmann et al. (2003) examined the effects of framing on decision-making behavior. Their study analyzed how antismoking messages in a wellbeing context could spur a person when posed by a risk involving the harmful effects of smoking. They found that negatively framed anti-smoking messages had more impact on people compared to positively framed messages

Past research also suggests that users tend to be more inclined towards pursuing risks, when they are presented with a case of financial losses which could affect the financial budget of the organization (Beebe et al., 2014). Beebe et al. (2014) surveyed industry professionals to understand their decision-making processes when responding to information security budget requests. The findings suggest that decision makers may be more inclined to take risks when presented with information security budget requests that emphasize the financial losses (i.e., negative framing) that will impact the organization if the budget requests are not met (Beebe et al., 2014).

The literature also indicates that users tend to show a high security behavior when they are given a message that focuses on the benefits of performing a secure action, rather than the negative outcomes of not performing it (Anderson & Agarwal, 2010). From the

findings of the study, the researchers found that users may perform cybersecurity actions depending on how the potential gains or potential losses that would result from the actions are presented to them (Anderson & Agarwal, 2010).

Research studies in the literature have examined the impact of message framing on various reliant variables covering intents (Block & Keller, 1995) and threat awareness (Lee & Aaker, 2003). Hence, we expect the cybersecurity behavior of users to be influenced by the way messages are framed (LaRose et al., 2008). Table 2.2 provides a summary of the literature on message framing.

Table 2.2. Summary of Literature Review on Message Framing

Reference	Description	Theory
Aaker & Lee (2001), Shiv et al. (2004)	Impact of positively expressed vs. negatively expressed messages on users' decision making. The authors found that negatively expressed messages had a significant impact on people's decision making compared to positively framed messages.	Prospect Theory
Beebe et al. (2014)	The authors examined the effect of negative framing of messages on users and how users tend to be more inclined towards pursuing risks when presented with a case of financial losses.	Prospect Theory

Table 2.2. Summary of Literature Review for Message Framing (cont.)

Reference	Description	Theory
LaRose et al. (2008)	The authors highlight individuals' responsibilities in a message to examine and optimize the users' cybersecurity behavior. The authors found that users' cybersecurity behavioral intentions can be further swayed by applying framing in messages.	Protection Motivation Theory and Social Cognitive Theory
Pechmann, et al. (2003)	The authors examined how antismoking messages in the wellbeing context could spur a person when posed by a risk involving the harmful effects of smoking.	Protection Motivation Theory
Tversky & Kahneman (1984)	The authors studied the impact of monetary losses and gains on users' behavior and found that users' perceived losses more seriously than gains.	Prospect Theory
Tversky & Kahneman (1986)	The authors analyzed the impact of message framing on individuals' behavior and their choices.	Prospect Theory

3. THEORETICAL FOUNDATION AND HYPOTHESES

To understand the cybersecurity behavior of users in monetary gain and loss scenarios, we draw on the Prospect Theory, which is one of the most widely used theories in economics. Prospect Theory is based on the economic principles of decision making under uncertainty (Fishburn, 1970; Kahneman & Tversky, 1979).

3.1. THEORETICAL FOUNDATION: PROSPECT THEORY

Prospect Theory provides insights about the decisions people make when they are under a state of threat or uncertainty, and where they are also aware of the probability of the outcome (Tversky & Kahneman, 1984). The choices that are made by people are based on their acumen, and the acumen which people perceive is based on the relative evaluation of the external factors of the world. Making choices are hard, and can be difficult for users who are confronted with risks, as it is difficult to predict the outcomes with certainty. Making choices can be strenuous from a user's perspective.

The process of decision-making by applying quantified risks as a metric involves two steps (McDermott, 1991). In the first step, the users assess risks by evaluating the vulnerabilities and by examining existing and possible hazards. The second step is about the influence on decision making, caused by the way in which information is presented or framed (McDermott, 1991).

Prospect theory mainly focuses on the process of decision making and how confined those decisions are. Decision-making based on prospect theory involves two phases. In the first phase, people assess the possible levels of risks involved in their given

choices based on their reference point (Tversky & Kahneman, 1984). The impact due to this subjective assessment is known as framing, in which a prospect is subjectively estimated as either a loss or a gain. This phase involves the organization and reformulation of all the possible options to simplify the process of evaluation and decision making (Tversky & Kahneman, 1984). After this phase, which involves the framing of all the alternatives based on the given conditions, each of the possible alternatives is assessed based on how they are perceived (either as gains or as losses). The choice with the highest benefit is then selected by the user. During the second phase, judgements made are loss aversive, i.e., people are more concerned about losses. The loss averse behavior indicates that losses are perceived stronger than gains (Verendel, 2009). Prospect theory indicates that users perceive a loss to be more substantial than a benefit of the same quantity (Tversky & Kahneman, 1986). Prospect theory also explains loss aversion, which suggests that users are more likely to react to losses than gains.

Tversky and Kahneman (1986), explain the outcome of people's decisions based on gains and losses in a value function. Figure 3.1 depicts the value function with value on the vertical axis and outcome on the horizontal axis. If we observe from the reference point (which is the point of origin of the axes), the value function in the loss condition is different from the value function in the gain condition. The value function for the loss condition shows a deeper curve, whereas the value function for the gain condition flattens horizontally at a smaller value.

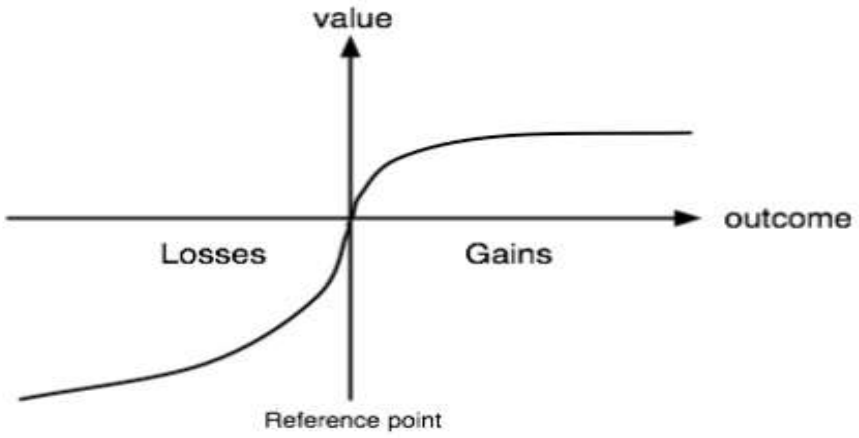


Figure 3.1. Prospect Theory

The value function is represented as a convex function for losses and a concave function for gains. It shows that people are more likely to seek risks to avoid losses, which is explained as loss aversion (Tversky & Kahneman, 1984). This loss aversion behavior indicates that people are more likely to take risks to avoid or minimize losses. The value function for the gain condition is a concave function, and it becomes parallel to the horizontal axis (outcome) after a certain value (Tversky & Kahneman, 1986). The value function for the gain condition shows that it curves at a lower value compared to the value function for the loss condition. Hence, people tend to be less risk seeking (i.e., more risk averse) when presented with a condition of receiving a gain than avoiding a loss (Tversky & Kahneman, 1986).

Tversky and Kahneman (1986) observed that the value function reaches a state of saturation or a state of diminishing sensitivity after reaching a certain value in the case of gains and losses as depicted in Figure 3.1. This point of saturation or diminishing sensitivity in the value function is the flattening of the value function in both the gain and

loss conditions. This point of diminishing sensitivity shows the change in the sensitivity of monetary benefits and losses observed among people.

3.2. HYPOTHESES

Prospect theory, which was first introduced in behavioral economics, plays an important role for generating the hypotheses for this research. Prospect theory states that people perceive losses more seriously than benefits of the same amount (Tversky & Kahneman, 1984).

Prospect theory explains behavior of people as loss aversion, where people try to minimize losses, even though the probability of experiencing losses is small. For example, Tversky & Kahneman (1984) conducted an experiment where the subjects were given a scenario where they had to make a decision regarding an outbreak of a disease that was estimated to kill 600 people. The options were: (A) 100% chance that 400 people will die, and (B) There is 1/3 probability that nobody will die, and a 2/3 probability that 600 people will die. 78% of the subjects chose option B over option A, which indicates that there is a preference towards the possible prevention of losing all 600 people rather than losing only 200 people with certainty. The results from this experiment indicates that people were more willing to take risks to avoid a loss. This risk seeking behavior was not observed when people were presented with scenarios involving a benefit or gain, as people show a risk adverse behavior when presented with scenarios involving a benefit compared to scenarios involving a loss.

Based on people's risk seeking behavior to avoid losses from prospect theory, this research applies the findings from prospect theory to study the behavior of users in a

scenario involving a cybersecurity risk. In cybersecurity related scenarios, the process of decision making for the users becomes even more complex as the users' decisions can be influenced by both the scenarios and framing of messages. Based on prospect theory, users are more likely to take a risky cybersecurity action to avoid a monetary loss as compared to receive a monetary gain. Hence, based on prospect theory, we propose the following hypothesis:

H1: Users are more willing to engage in risky computer security behavior to avoid a loss than to receive a gain.

In this research, we draw on the principle underlying the value function (see Figure 3.1) from prospect theory in the field of economics by Tversky and Kahneman (1986) and apply it to cybersecurity scenarios. To understand user behavior in a cybersecurity scenario, we propose to examine the point at which users show a different cybersecurity behavior in both the gain and loss scenarios. We call this point the tipping point based on the expected monetary value. Hence, the tipping point refers to the expected monetary value below which users will not be risk seeking. In other words, the tipping point is the maximum expected monetary value in which users show a risk averse behavior and are willing to take risks. Prospect theory also explains that people tend to be more concerned about damage or monetary losses than monetary benefits and that people show a risk seeking behavior to avoid a loss (Tversky & Kahneman, 1986). We propose that based on prospect theory, users show a change in their cybersecurity behavior at a lower value to avoid a monetary loss than to receive a monetary gain, as they perceive the impact of a loss more seriously than a gain of the same monetary value. Similarly, in the case of a monetary

gain, users show a change in their cybersecurity behavior at a higher value than the case of a monetary loss, as the findings of prospect theory show that people are more risk averse when they are experiencing a gain or a benefit.

Hence, based on the explanation provided by prospect theory on the value function, user behavior, and how the user behavior changes based on expected monetary value, we propose the following hypothesis:

H2: Users exhibit a higher tipping point of expected monetary value to engage in risky computer security behavior when receiving a gain than avoiding a loss.

Tversky and Kahneman (1986) explain that the value function is normally concave above the reference point when there is a gain and the value function is often convex below the reference point in the case of a loss (see Figure 3.1). Prospect theory also suggests that the value function is steeper for losses than for gains (Tversky & Kahneman, 1986). This steepness in the convex function shows the loss aversion observed among people when given a loss condition.

Prospect theory also indicates that the way in which people perceive guaranteed conditions is different from the way in which people perceive probable conditions (Tversky & Kahneman, 1986). When presented with conditions that have a 50% probability of a loss, it was observed that majority of people perceive it as a 50% probability of not incurring a loss. It shows the risk seeking behavior of people as explained in prospect theory (Tversky & Kahneman, 1986). Based on findings from prospect theory, people tend to prefer a probable loss over a guaranteed or certain monetary loss even when controlling for the expected value of the loss (Tversky & Kahneman, 1986). This behavior is due to

the way in which the conditions are perceived. Individuals tend to perceive the probable factor more seriously than the guaranteed factor in the loss scenario, which is in line with loss aversion in prospect theory. In perceiving the probable factor, people tend to give importance to the chance for a significant loss in the outcome. This probability for a change in the outcome associated with a monetary loss takes precedence when compared to a guaranteed monetary loss even though the expected monetary value is the same (Tversky & Kahneman, 1986). The following example illustrates this loss averse behavior.

Example: In addition to whatever people own, they have been given $2000, and they were asked to choose between two choices: i) A 50% probability that they lose $1000, and ii) A 100% probability that they lose $500. For the above condition, 69% of them chose the first choice of taking a 50% chance of losing $1000 (Tversky & Kahneman, 1986). In the example, the expected monetary value in the probable and guaranteed conditions have the same expected outcome, as 50% of $1000 is $500, and 100% of $500 is also $500. The findings suggest that individuals preferred the risk seeking option because they saw an opportunity for change (i.e., avoid a huge loss) in the outcome as compared to the outcome with certainty, even though the expected monetary value outcome remains the same in both the conditions (Tversky & Kahneman, 1986). Prospect theory indicates that users perceive a probable loss to be more substantial than a certain or guaranteed loss of the same quantity, i.e., probable damage is favored over a guaranteed damage (Tversky & Kahneman, 1986).

Based on prospect theory, when users are presented with a scenario involving a risky cybersecurity choice, they would rather face a probable loss over a guaranteed loss when controlling for the expected loss (Tversky & Kahneman, 1986). In other words, users

are more willing to take a risky cybersecurity action to avoid a guaranteed loss over a probable loss when the amount of expected loss is controlled due to their preference for experiencing a probable loss over a guaranteed loss. Hence, users show risk seeking behavior, as they tend to perceive the probability of experiencing a monetary loss more importantly as the probability of not experiencing or avoiding a monetary loss. Hence, based on prospect theory, the following hypothesis is proposed:

H3: Users are more willing to engage in risky computer security behavior to avoid a guaranteed loss than a probable loss, controlling for the amount of expected loss.

In assessing prospect theory, Kahneman and Tversky observed a risk averse behavior among the participants of their experiments when they were presented with scenarios involving a benefit or gain (Tversky & Kahneman, 1986). People prefer the choice with a higher probability of gaining a monetary benefit of a smaller value to the choice with a lesser probability of gaining a monetary benefit of higher value, with the expected utility controlled (Tversky & Kahneman, 1986). The following example from a study by Tversky and Kahneman (1986) illustrates human decision-making preference in the gain scenario.

Example: In addition to whatever you own, you have been given $1000, and the participants were asked to choose between two choices: i) There is a 50% probability of getting $1000 and, ii) There is a 100% probability of getting $500. 70% of the participants chose the second choice, thereby being risk averse when experiencing a gain (Tversky & Kahneman, 1986). It is explained in prospect theory that individuals show a risk averse behavior by preferring a guaranteed gain to a probable gain, even when the expected

monetary value is the same, given that they prefer receiving $500 with certainty, rather than taking the risk of either getting $1000 or not getting $1000.

As explained in the above example that is based on prospect theory, people prefer receiving a monetary benefit of a smaller amount with certainty to the probability of receiving a larger monetary benefit (Tversky & Kahneman, 1986). Based on the findings from prospect theory and applying it in a cybersecurity scenario, we propose that users are more likely to carry out a risky cyber security action to obtain a monetary benefit or gain with certainty as compared to a probability of receiving a monetary benefit with the same expected gain (Tversky & Kahneman, 1986). Hence, people are risk adverse when faced with gains. Based on prospect theory, we propose the following hypothesis:

H4: Users are more willing to engage in risky computer security behavior to receive a guaranteed gain than a probable gain, controlling for the amount of expected gain.

Based on prospect theory and Figure 3.1 that shows the value function, the tipping point value (monetary value above which the user would perform a cybersecurity action to prevent a loss or receive a gain) between probable and guaranteed gains and losses is compared. By applying prospect theory in a cybersecurity context, we expect users to prefer a probable monetary loss to a guaranteed monetary loss with the same expected loss (Tversky & Kahneman, 1986). In other words, users' preference is to avoid a guaranteed loss over a probable loss of the same expected loss. As users prefer a probable monetary loss to a guaranteed monetary loss, they will show a change in their risk-taking behavior (tipping point) at a higher monetary value in the probable monetary loss condition as compared to the guaranteed monetary loss condition. Similarly, when presented with

guaranteed and probable gain scenarios that control for the amount of expected gain, users are more likely to take a risky cybersecurity action in the guaranteed monetary gain condition as compared to the probable monetary gain condition because users are risk adverse with gains (Tversky & Kahneman, 1986). Hence, in both the gain and loss contexts, we expect users to show a change in their cybersecurity behavior (tipping point) at a higher monetary value in the probable condition than the guaranteed condition (Tversky & Kahneman, 1986). To hypothesize the difference in the tipping point between guaranteed and probable conditions, we propose the following:

H5: Users are more willing to engage in a risky computer security behavior at a higher tipping point of expected monetary value in the probable condition as compared to the guaranteed condition in both gain and loss scenarios.

4. RESEARCH METHODOLOGY

This section covers the experimental design, research procedures, measurement, and pilot tests to assess the hypotheses proposed in section 3.

4.1. EXPERIMENTAL DESIGN

A 2 X 2 between-subjects experimental design was used to test the hypotheses: H1, H2, H3, H4 and H5. The first factor is Monetary Polarity, which has two levels, Gain and Loss. The second factor is Certainty, which has two levels, Guaranteed (100%) and Probable (50%). Hence, the four experimental conditions are: (i) Guaranteed Gain, (ii) Guaranteed Loss, (iii) Probable Gain, and (iv) Probable Loss. Subjects were randomly assigned to one of the four experimental conditions. To assess the tipping point of each subject in their assigned experimental condition, a repeated measure within the 2 X 2 design was used. This repeated measure was operationalized using Expected Monetary Value of the gain or loss in the four conditions. Controlling for Expected Monetary Value, the starting value was set to $100 in all four conditions. Hence, the guaranteed conditions (Guaranteed Gain and Guaranteed Loss) were associated with a starting value of $100 gain and loss, and the probable conditions (Probable Gain and Probable Loss) were associated with a starting value of a 50% chance of a gain or loss of $200, resulting in an expected value of a gain or loss of $100. In other words, the reason behind setting the starting value at $100 for guaranteed conditions and $200 for probable conditions is that the Expected Monetary Value is equal to $100 in both cases, since the probable conditions have a 50%

chance of gaining or losing $200. In other words, 50% chance of gaining/losing $200 will have an Expected Monetary Value of 0.5 * $200 = $100.

If the subject indicates that he or she will not take the cybersecurity risk in the first scenario (i.e., expected monetary value of $100), then the tipping point is $100 (or more). If the subject indicates that he or she will take the cybersecurity risk in the first scenario, then scenarios with expected monetary values of $75, $50 and $25 follow until the subject chooses not to take the cybersecurity risk. In other words, if the subject indicates that he or she will not take the cybersecurity risk at one of the three expected monetary values of $75, $50 or $25, we have identified the tipping point to be in the range of $75-$100 (if the subject indicates so when presented with an expected monetary value of $75), $50-$75 (if the subject indicates so when presented with an expected monetary value of $50) or $25-$50 (if the subject indicates so when presented with an expected monetary value of $25). If the subject indicates that he or she will take the cybersecurity risk at all three levels of expected monetary values of $75, $50, and $25, then the tipping point falls in the range of $0-$25.

In the case where the tipping point was found to be in the range of $75-$100, $50-$75 or $25-50, we increase the expected monetary value by $5 in the next four scenarios until the subject indicates that he or she will take the cybersecurity risk. If the tipping point falls in the interval of $0-$25, four possible scenarios with expected monetary values of $5, $10, $15, and $20 are to be presented until the subject indicates that he or she will take the cybersecurity risk, which suggests that the tipping point was reached. Finally, the subject will also be asked if he or she will take the cybersecurity risk when expected

monetary value of zero is encountered. If the subject indicates yes, the tipping point is zero. Figure 4.1 shows the logic and ordering of the scenarios presented to the subjects.

Unless the tipping point is zero, it is computed as the average of the $5 interval below the lowest (non-zero) expected monetary value in which a risky cybersecurity action was undertaken. If a subject indicates that he or she will take the cybersecurity risk at the expected monetary value of $100 and then indicates that he or she will not take the cybersecurity risk at expected monetary value $95, then the average in the $5 interval is $97.5, which is the tipping point. The series of scenarios presented to the subjects end with a scenario with expected monetary value of zero.

The cybersecurity risk in the experiment involved downloading a software application called “Ad-hoc Pro” from an uncertified developer. This software application provides an ad free browsing experience that no software in the market can provide. However, because the developer is uncertified, there is a risk involved in downloading the software application.

Based on the monetary value gain or loss scenario posed to the subjects, they made a decision whether to download or not download the “Ad-Free Pro” software application.

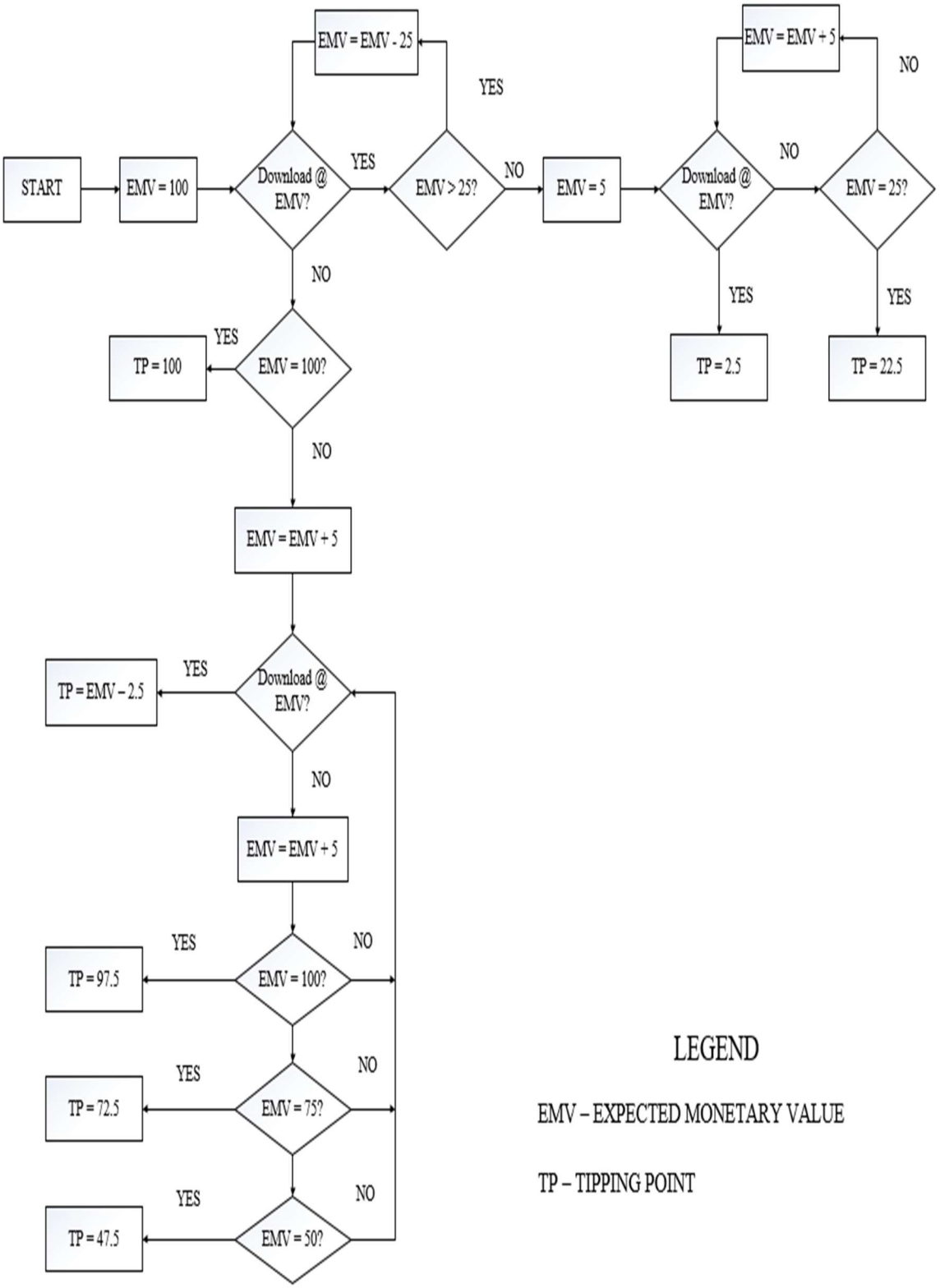


Figure 4.1. Logic of Experimental Scenarios

4.2. RESEARCH PROCEDURES

The experimental study was conducted in the computer labs at the Missouri University of Science and Technology. The opening scenario that was presented to all subjects at the beginning of the experiment is shown in Appendix A. The scenario indicates that all subjects were presented with $200 free credits and were asked to download an ad-free software application from an uncertified developer. Subjects were then presented with a series of scenarios and had to made decisions on whether to download or not download the software application based on the monetary condition presented in each scenario. Appendix B shows the first scenario associated with each of the four experimental conditions: Guaranteed Gain, Guaranteed Loss, Probable Gain, and Probable Loss. The experimental scenarios were operationalized based on the Expected Monetary Value of $100 for the first scenario. The subjects were presented with scenarios in guaranteed or probable condition involving either a monetary gain or monetary loss and asked to make a choice to download or not download the application from the uncertified developer. In each scenario, validation check questions were included to make sure subjects understood the given scenario before making the decision of downloading or not downloading the "Ad-Free Pro" application from an uncertified developer. The subjects were also asked to explain their rationale behind choosing to download or not download the application. The subjects were then presented with manipulation check questions as shown in Appendix C, and that were used to check if the subjects had understood and paid attention to the scenario details.

After answering the manipulation check questions (Appendix C), the subjects were presented with a control scenario based on the same experimental condition and asked

whether they would download the "Ad-Free Pro" application from the uncertified developer from whom the subject had received $200 worth of free Amazon shopping credits. The control condition is provided in the Appendix D. It involved no monetary polarity (no loss or gain). The control condition is used in this experimental study to validate the certainty and authenticity of the subject's choices made in all the experimental scenarios.

After completing the control condition question, the subjects were presented with a questionnaire with questions on a 7-point Likert's scale to examine the perceptual outcomes of the subjects (Threat Severity, Trust, Importance of Primary Computer, and Tolerance towards Ads).

The questionnaire to examine the perceptual outcomes of the subjects is provided in Appendix E. The questions were randomized and presented by the system to all the subjects to prevent any ordering effect.

After completing the questionnaire to examine the perceptual outcomes, the subjects were presented with the background and demographics questionnaire, which is provided in Appendix F. The questionnaire consists of questions examining the subject's gender, age, race, internet usage and software download frequency. After completing the background and the demographics questionnaire, the subjects were presented with a cyber-security awareness questionnaire which is provided in Appendix G. The cybersecurity awareness questionnaire is adopted from a cybersecurity awareness survey by Manjak (2006). The questions in the cybersecurity awareness questionnaire were also randomized by the system to prevent any ordering effect. The subjects were provided with a comments

section after completing the cybersecurity awareness questionnaire, where they could share their comments or feedback about participating in this experimental study.

4.3. MEASUREMENT

After completing the experimental conditions, the subjects were presented with a post-study questionnaire, which was used to assess if the subject was currently using his/her primary computer, if the subject stores all his important files in the cloud, and perceptual outcomes associated with user actions, i.e., importance of primary computer, fear, threat severity and, trust. The post-study questionnaire included manipulation check questions and other check questions, to validate each subject's understanding of the questions and attention to these questions. The demographics and the information about the subject's understanding of cybersecurity were recorded using measurement items in the post-study questionnaire.

4.3.1. Importance of Primary Computer. The importance of the primary computer scale was developed by the researcher and used to assess the importance that the subject possesses for his/her primary computer. This measurement is used to examine and understand the decision of subjects to download or not download the "Ad-Free Pro" application. To collect the responses from the subjects, a 7-point Likert scale (strongly disagree=1 to strongly agree=7) was used. The measurement items used in this research study to examine the importance of primary computer among users is explained in Table 4.1.

Table 4.1. Measurement Scale for Importance of Primary Computer

	Measurement Items
Importance of Primary Computer (IPC)	(IPC1) I have important files stored on my primary computer.
	(IPC2) My primary computer is valuable to me.
	(IPC3) The data on my primary computer is important to me.
	(IPC4) I cannot afford to lose the files on my primary computer.
	(IPC5) I will not risk the security of my primary computer.
	(IPC6) My primary computer is very important to me.

4.3.2. Threat Severity. Threat severity refers to the level of severity of the threat perceived by the subject regarding downloading a software from the Internet. The measurement items (see Table 4.2), were adopted from Johnston and Warkentin (2010) in which they explain that the factor, threat severity, assesses the degree of danger associated with a cybersecurity threat. To collect the responses from the subjects, a 7-point Likert scale (strongly disagree=1 to strongly agree=7) was used.

Table 4.2. Measurement Scale for Threat Severity (Johnston & Warkentin, 2010)

	Measurement Items
Threat Severity (TS)	(TS1) If my computer were infected by malware because of downloading the "Ad-Free Pro" application, it would be severe.
	(TS2) If my computer were infected by malware because of downloading the "Ad-Free Pro" application, it would be serious.
	(TS3) If my computer were infected by malware because of downloading the "Ad-Free Pro" application, it would be significant.

4.3.3. Trust. Trust is personality trait which is defined as a person's inclination to believe in an action (Freed, 2014). The measurement items (see Table 4.3) for trust were adopted from Freed (2014), to assess the level of trust that an individual user possessed on a software provider. To collect the responses from the subjects, a 7-point Likert scale (strongly disagree=1 to strongly agree=7) was used.

Table 4.3. Measurement Scale for Trust (Freed, 2014)

	Measurement Items
Trust (T)	(T1) I believe the "Ad-Free Pro" application is a trustworthy application.
	(T2) I trust the vendor of the "Ad-Free Pro" application.
	(T3) I trust the "Ad-Free Pro" application.

4.3.4. Fear. Fear is defined as an emotion that arises due to an anxiety of believing something or someone could cause harm (Freed, 2014). The measurement of the fear factor was adopted from Freed (2014) to assess the level of fear possessed by the subjects on downloading "Ad-Free Pro" application from the Internet (see Table 4.4). The study by Freed (2014) explains that fear is caused by past incidents related to cybersecurity threats. To collect the responses from the subjects, a 7-point Likert scale (strongly disagree=1 to strongly agree=7) was used.

Table 4.4. Measurement Scale for Fear (Freed, 2014)

	Measurement Items
Fear(F)	(F1) I was worried about downloading the "Ad-Free Pro" application.
	(F2) I was concerned about downloading the "Ad-Free Pro" application.
	(F3) I experienced fear when deciding if I should download the "Ad-Free Pro" application.

4.3.5. Tolerance towards Ads. Tolerance towards ads was used to examine the subject's ability to bear with the interruptions caused due to ads while browsing the Internet. Tolerance towards ads was measured in this experimental study to assess if there is an effect of the subject's tolerance towards ads on his/her decision to download or not download the "Ad-Free Pro" application. The researcher developed the measurement items for tolerance towards Ads (see Table 4.5). To collect the responses from the subjects, a 7-point Likert scale (strongly disagree=1 to strongly agree=7) was used.

Table 4.5. Measurement Scale for Tolerance towards Ads

	Measurement Items
Tolerance towards Ads (TA)	(TA1) I hate having ads on my primary computer.
	(TA2) Having ads on my primary computer is fine with me.
	(TA3) I am bothered by ads on my primary computer.
	(TA4) I like to have ads on my primary computer.
	(TA5) I do not mind having ads on my primary computer.
	(TA6) I do not want ads on my primary computer.

4.3.6. Manipulation Check. The manipulation check questions assessed the understanding of the subjects about the monetary gain or loss condition that the subject experienced as well as the certainty level associated with the gain or loss. The researcher developed the measurement items for the manipulation check (see Table 4.6). The items were included to assess the effectiveness of the experimental manipulations and to analyze if the subjects had understood the scenario details and the experimental conditions. Subjects answered the first manipulation check question (see Table 4.6) on a Gain / Loss binary scale and answered the second manipulation check question by selecting the probability (0%, 50% and 100%) among the options given to them.

Table 4.6. Measurement Scale for Manipulation Check

	Measurement Items
Manipulation Check	(MC1) In the scenarios above, on downloading the "Ad-Free Pro" software, you experience a _____
	(MC2) In the scenarios above, on downloading the software, what are your chances of experiencing a gain/loss?

4.3.7. Demographics and Subject's Background Questionnaire. The survey questionnaire to assess the subject's demographic and background information (Appendix F) contains items on the subject's demographics that include gender, age, education level, and occupation. The questionnaire also includes items to assess the Internet usage and the frequency of software downloads from the Internet.

4.3.8. Cybersecurity Awareness Questionnaire. The measurement items for cybersecurity awareness (Table 4.7), that are provided in Appendix G were adopted from a cybersecurity awareness survey by Manjak (2006). The cybersecurity awareness questionnaire was included in this experimental study to assess awareness about basic cybersecurity practices and the threats in the domain of cybersecurity.

Table 4.7. Measurement Scale for Cybersecurity Awareness (Manjak, M., 2006)

	Measurement Items
Cybersecurity Awareness (CySA)	CySA1- I am careful when downloading third-party software.
	CySA2- I often download from third party websites. (Reversed)
	CySA3- My computer often gets infected by viruses. (Reversed)
	CySA4 - I do not use anti-virus software on my computer.
	CySA5 - I frequently update the anti-virus software on my computer.
	CySA6 - I have anti-virus software installed, updated, and enabled on my computer.
	CySA7- I often download and install unlicensed software. (Reversed)

4.3.9. Check Questions. Check questions were included in the questionnaire to examine if the subject is attentive in answering the questions presented to them during the experimental study. The measurement items for the check questions were developed by the researcher (see Table 4.8). To collect the responses from the subjects and to maintain consistency with the rest of the questions in the survey, a 7-point Likert scale (strongly disagree=1 to strongly agree=7) was used.

Table 4.8. Measurement Scale for Check Questions

	Measurement Items
Check Questions (CHK)	(CHK1) Please check "Strongly Agree".
	(CHK2) Please check "Strongly Disagree".

4.4. PILOT TESTS

Three pilot tests were carried out. The comments from the participants of the first pilot study were used to revise the experimental conditions and evaluate the measurement items. Some of the measurement items and the scenario details were not easily understandable and were complex, which were rephrased to a more understandable form. The feedback from the participants of the second pilot study was used to correct the experimental procedures and the logical flow of the experimental study.

After the third pilot study, the comments from the participants were used to correct the way in which the measurement items were presented to the subjects, thereby making the post-study questionnaire more understandable. Since there were many measurement items, we decided on adding check questions which helped us assess if the subjects were attentive when responding to the questionnaire.

5. DATA ANALYSIS

The graduate and undergraduate students from the Business and Information Technology department of Missouri University of Science and Technology participated in the experiment. The total number of subjects who participated in the study was 151. After removing the data points that did not pass the manipulation check questions or the check questions in the post-study questionnaire, the sample size is 120. The sample for this experimental study had both male and female subjects who were sourced to participate in this experimental study through the help of professors of classes and through email contact.

In this chapter, the demographic information of the subjects will be presented and the reliability and validity of the measurement will be assessed. H1, H3, and H4 will be assessed using multinomial logistic regression analysis and the chi-square test, as both are appropriate tests for them. Multinomial logistic regression and Chi-Square tests are methods used to statistically analyze and predict binary or categorical outcomes. The difference between these two methods is that the multinomial logistic regression method predicts the response or dependent variable as binary outcomes, whereas chi-square method provides the descriptive statistics of the categorical variables. Since the dependent or response variable is dichotomous (i.e., download or not download), multinomial logistic regression and chi-square analysis are used to validate the hypotheses H1, H3 and H4. H2 and H5 will be assessed using the univariate analysis of variance method. The univariate analysis of variance method is used to examine the relationship or interaction existing between the factors and the dependent variable, i.e., between the two independent variables, monetary polarity and certainty, and the dependent variable, tipping point.

5.1. DEMOGRAPHIC INFORMATION OF SUBJECTS

The demographic information of the subjects is summarized in Table 5.1. The participants of this experimental study fall in the age group of 18 to 44. The factor analysis, and the validity and reliability analysis of measurement were also conducted. IBM SPSS Statistics 11.0 software was utilized to cleanse and analyze the data that was collected during the experimental study.

Table 5.1. Summary of Demographic Details of Subjects

Gender	
Male	58.30%
Female	41.70%
Age	
18-24	82.50%
25-34	11.70%
35-44	1.70%
45-54	0.00%
55-64	0.00%
65-74	0.00%
75 or older	0.00%
Race and Ethnicity	
White	63.30%
Black or African American	7.50%
American Indian or Alaskan Native	0.00%
Asian	20.80%
Native Hawaiian or Pacific Islander	0.80%
Hispanic or Latino	4.20%

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

Other	2.50%
Prefer Not to Disclose	0.80%
Marital Status	
Single	89.20%
Married	10.00%
Widowed	0.00%
Divorced	0.80%
Separated	0.00%
Time Spent Online (Per Week)	
1-5 hours	1.70%
6 - 10 hours	11.70%
11-15 hours	17.50%
16-20 hours	24.20%
20+ hours	45.00%
Frequency of Software Download from the Internet?	
Rarely Never	48.30%
Once a Month	21.70%
Two or Three Times a Month	18.30%
Four Times or More Than Four Times a Month	11.70%
Major Field of Study	
Information Science and Technology	50.00%
Business and Management	40.00%
Engineering	2.50%
Psychology	2.50%
Other (Please Specify)	5.00%
Student Level	
Undergraduate Student	79.20%
Graduate Student	19.20%
Certificate-Seeking (only) Student	0.80%
Other (Please Specify)	0.80%
Employment Status	
Working (Paid Employee)	41.70%
Working (Self-Employed)	3.30%

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

Not Working	50.80%
Prefer Not to Disclose	4.20%
Family Income (Previous Year, Before Taxes)	
Less than $10,000	10.00%
$10,000 to $49,999	19.20%
$50,000 to $99,999	37.50%
$100,000 to $149,999	20.00%
$150,000 or More	13.30%
Disposable Income (Per Month)	
Less Than $100	35.00%
$100 - $500	43.30%
$501 - $1000	10.80%
$1001 - $2000	5.80%
More Than $2000	5.00%

5.2. MEASUREMENT VALIDATION

The convergent and discriminant validity for the measures in the post-study questionnaire were analyzed using the Exploratory Factor Analysis (EFA) method. The values of varimax rotation and principal component analysis of EFA are reported in Table 5.2 and Table 5.3.

A 9 X 9 factorial structure was created consisting of eigenvalues (>1.0). The target factors were loaded by the respective measurement items in all the cases except the measurement items for cybersecurity awareness as they are formative unlike other measures that are reflective.

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

	1	2	3	4	5	6	7
TA2	.866	-.044	.028	-.149	-.113	.083	.081
TA5	.863	-.078	.033	-.108	-.107	.107	.049
TA1	.824	-.225	-.034	.025	.027	.046	.004
TA4	.795	.192	.178	-.128	-.026	-.030	-.181
TA6	.786	-.053	.071	.051	.050	.133	.096
TA3	.658	-.081	-.056	.206	.094	-.137	-.083
IPC1	-.059	.830	-.061	.218	.010	.091	-.056
IPC3	-.056	.797	-.154	.210	.099	-.068	-.005
IPC4	-.118	.765	.003	.147	.094	.137	-.214
IPC6	-.027	.729	-.033	.086	.135	-.025	.477
IPC2	-.073	.709	.001	.002	.108	.097	.479
IPC5	-.041	.688	-.220	.305	-.078	.163	.184
T3	.064	-.060	.903	-.080	-.045	-.154	-.039
T1	.060	-.090	.880	-.118	.060	-.140	-.122
T2	.105	-.142	.855	-.161	-.071	-.109	-.181
TS1	-.104	.224	-.143	.842	.004	.088	.063
TS2	-.061	.249	-.070	.826	-.041	.190	.113
TS3	.054	.302	-.167	.790	.013	.157	.054
CySA6	-.024	.100	.019	-.009	.896	.036	-.006
CySA5	-.100	.140	.001	.012	.878	.059	.148
CySA4	.068	-.009	-.089	-.043	.868	.009	.015
F3	-.006	.029	.006	.149	-.030	.779	-.116
F1	.128	.111	-.424	.120	.173	.700	-.102
F2	.067	.090	-.579	.091	.071	.641	.020
CySA2	.142	.113	-.162	.206	-.044	.517	.385
CySA7	.123	.118	-.117	.464	-.108	.508	.348
CySA1	-.026	.060	-.199	-.019	.269	.484	.423
CySA3	-.008	.059	-.177	.168	.075	-.045	.752

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 7 iterations.

Legend: TA: Tolerance towards Ad; IPC: Importance of Personal Computers; T: Trust; F: Fear; CySA: Cybersecurity Awareness

Table 5.3. Results of Factor Analysis (after removing TA3 and IPC2)

	1	2	3	4	5	6	7
TA5	.882	-.083	.021	-.078	-.091	.063	.063
TA2	.881	-.050	.016	-.115	-.095	.039	.081
TA4	.823	.181	.158	-.077	-.001	-.052	-.208
TA6	.806	-.077	.047	.110	.075	.076	.069
TA1	.805	-.226	-.032	.025	.026	.040	.021
IPC1	-.055	.859	-.046	.186	.007	.093	.020
IPC3	-.066	.808	-.144	.191	.102	-.062	.014
IPC4	-.109	.808	.022	.100	.085	.158	-.105
IPC5	-.044	.684	-.221	.306	-.073	.131	.213
IPC6	-.028	.669	-.055	.141	.161	-.084	.385
T3	.071	-.063	.902	-.075	-.041	-.143	-.063
T1	.060	-.089	.883	-.123	.058	-.110	-.135
T2	.109	-.138	.860	-.170	-.076	-.074	-.181
TS2	-.065	.243	-.078	.842	-.035	.151	.122
TS1	-.125	.224	-.143	.841	.005	.070	.067
TS3	.033	.296	-.172	.802	.019	.138	.052
CySA7	.141	.107	-.131	.489	-.101	.425	.410
CySA6	-.020	.097	.016	-.006	.900	.031	.001
CySA5	-.107	.134	.001	.010	.880	.049	.150
CySA4	.052	-.019	-.091	-.039	.869	.015	.000
F3	.000	.022	.002	.163	-.042	.802	-.035
F1	.132	.097	-.435	.148	.170	.709	-.049
F2	.085	.083	-.592	.118	.073	.616	.083
CySA3	-.008	.074	-.168	.147	.084	-.148	.782
CySA2	.162	.145	-.155	.180	-.049	.438	.530
CySA1	-.034	.066	-.188	-.039	.260	.459	.498

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 6 iterations.

Legend: TA: Tolerance towards Ad; IPC: Importance of Personal Computers; T: Trust; F: Fear; CySA: Cybersecurity Awareness

The measurement items listed in above show good convergent and discriminant validity (Cook & Campbell, 1979), except in the case of the measurement items TA3 and IPC2 which did not load as well. As shown in the results of the first factor analysis, IPC2 cross loaded with cybersecurity awareness and TA3 loaded much less on the factor than the rest of the items. Hence, both items were dropped. The EFA was once again carried out and the factor analysis. Table 5.3 provided the varimax rotated component matrix of results of EFA without items TA3 and IPC2.

Table 5.4. Results of Reliability Analysis

Construct	**Cronbach's alpha coefficient**
Tolerance Towards Ads (TA)	0.895
Importance of Primary Computers (IPC)	0.862
Trust (T)	0.918
Threat Severity (TS)	0.884
Fear (F)	0.774
Cybersecurity Awareness (CySA)	0.702

After completing the factor analysis of all the measurement items, the reliability analysis was performed to examine and calculate the Cronbach's alpha coefficients (Cronbach, 1951). The Cronbach's alpha coefficient (Cronbach, 1951) has been used as a

standard to assess internal consistency or reliability. The Cronbach's alpha coefficient value for the seven factors are provided in Table 5.4.

Cronbach's alpha coefficient of a minimum of 0.70 indicates a good reliability of the constructs (Nunnally, Bernstein, & Berge, 1967). The Cronbach's alpha coefficients shown in Table 5.4 are well above 0.7, suggesting that all the measures and their respective measurement components are reliable.

5.3. MULTINOMIAL LOGISTIC REGRESSION ANALYSIS

Multinomial Logistic Regression is a method used to statistically analyze and predict binary outcomes. The binary or categorical outcomes that are predicted using this method are dichotomous i.e., having only two possible values such as 0's and 1's or Yes/No. Multinomial logistic regression is a method of regression analysis where nominal outcome variables are modelled. In this type of logistic regression, the log odds of the variables are modelled as dependent variables, in a linearly combined form.

Multinomial Logistic Regression is used to develop and analyze a model with the factor and the covariates. Multinomial Logistic Regression is generally applied where the dependent variables are binary variables like in this case where we analyze whether the subjects have chosen to download the "Ad-Free Pro" application or not across the guaranteed gain, guaranteed loss, probable gain, and probable loss conditions. Also, the covariates include Importance of Primary Computer, Threat Severity, Trust, Fear, Tolerance towards Ads, and Cyber Security Awareness. We also analyzed the multinomial logistic regression on the download action for scenarios operationalized using Expected

Monetary Values $100. The results of the binary logistic regression for expected monetary value $100 are reported in Table 5.5. The variables represented in following table are:

- **B.** The value of B is the logistic coefficient that represents the relationship exhibited by the independent variables, Monetary Polarity (Gain vs Loss) and Certainty (Guaranteed vs Probable).

- **S.E.** The variable S.E. represents Standard Error. The value provided under the S.E column is used to examine if the value of the parameter is largely different compared to 0. The t-value is calculated by dividing the parameter estimate by the value of the standard error. The confidence intervals for the parameters are created based on the value of the standard errors.

- **Wald and Sig.** The Wald chi-square value and 2-tailed p-value are used to test if the value of the null hypothesis is 0. For our data analysis, we will compare each p-value to our preselected alpha threshold of 0.05. Coefficients that have a sig value (p-value) lesser than the preselected alpha value are considered to be statistically significant (Peng, Lee, & Ingersoll, 2002).

- **Degree of Freedom (df).** The variable, df, represents the degree of freedom of the coefficients for a particular test.

- **Exp(B).** The odds ratio of the predictor variables is reported under the Exp(B) column in Table 5.5. The odds ratio is computed by applying the exponentiation operation on the values of the coefficients. The values show the possibility of a particular event happening with respect to the reference variable.

Table 5.5. Results of Multinomial Logistic Regression Analysis for Expected Monetary Value of $100

Download for $100		B	Std. Error	Wald	df	Sig.	Exp(B)	95% Confidence Interval for Exp(B) Lower Bound	95% Confidence Interval for Exp(B) Upper Bound
0	Intercept	-7.928	2.825	7.877	1	.005			
	Importance of Primary Computer	.496	.341	2.117	1	.146	1.643	.842	3.205
	Threat Severity	.503	.292	2.969	1	.085	1.654	.933	2.931
	Trust	-.902	.237	14.478	1	.000	.406	.255	.646
	Fear	.267	.256	1.085	1	.298	1.306	.790	2.156
	Tolerance towards Ads	.278	.248	1.256	1	.262	1.321	.812	2.148
	Cyber Security Awareness	.661	.311	4.521	1	.033	1.936	1.053	3.560
	Loss [Monetary Polarity=0]	-.331	.510	.421	1	.517	.718	.264	1.952
	Gain [Monetary Polarity=1]	0[b]	.	.	0	.	.	.	.
	Probable [Certainty=0]	-.631	.530	1.420	1	.233	.532	.188	1.503
	Guaranteed [Certainty=1]	0[b]	.	.	0	.	.	.	.

a. The reference category is: 1.

b. This parameter is set to zero because it is redundant.

Monetary Polarity. From the results of the analysis as shown in Table 5.5, we found that the variable Loss ($p = 0.517$) does not show any significant effect in influencing the outcome to download or not download the software application over the Gain condition. The p-value is greater than the preselected alpha value of 0.05. Based on the value of

significance observed in the results of multinomial logistic regression, we conclude that monetary polarity has no significant effect on users' risky cybersecurity action. Hence, H1 is not supported.

Certainty. From the results of the analysis, we found that the variable Probable ($p = 0.233$) does not show any significant effect influencing the outcome of download or not download the software application over the Guaranteed condition. The p-value is greater than the preselected alpha value of 0.05. Based on the value of significance observed in the results of the analysis, we conclude that there is no significant difference in the effect of probable and guaranteed conditions on users' risky cybersecurity behavior.

Importance of Primary Computer (IPC). From the results of the analysis shown in results of multinomial logistic regression, we found that Importance of Primary Computer ($p = 0.146$) does not show any significant effect on the download outcome.

Threat Severity (TS). From the results of the analysis, we found that threat severity ($p = 0.085$) does not show any significant effect on the download outcome.

Trust (T). From the results of the analysis, we found that trust ($p < 0.05$) has a significant effect on the download outcome. Based on the significance observed in the analysis, we conclude that the covariate Trust has a significant effect on users' risky cybersecurity action.

Fear (F). From the results of the analysis shown in results of the multinomial logistic regression, we found that fear ($p = 0.298$) does not show any significant effect on the download outcome.

Tolerance towards Ads (TA). From the results of the analysis shown in results of multinomial logistic regression, we found that Tolerance towards Ads ($p = 0.262$) does not show a significant effect on the download outcome.

Cybersecurity Awareness (CySA). From the results of the analysis, we found that Cybersecurity Awareness ($p = 0.033$) has a significant effect on the download outcome. Based on the significance observed in the results from the multinomial logistic regression analysis, we conclude that the covariate, Cybersecurity Awareness, has a significant effect on the users' risky cybersecurity action.

To address H3 and H4, we conduct Multinomial Logistic Regression by assessing the effect of probable and guaranteed loss conditions on risky cybersecurity behavior separately from analyzing the effect of probable and guaranteed gain conditions on risky cybersecurity behavior.

From the results of the analysis as shown in the Table 5.6, we found that the variable Guaranteed ($p = 0.484$) does not show any significant effect in influencing the outcome to download or not download the software application over the Probable condition in a Loss scenario. The p-value is greater than the preselected alpha value of 0.05 (see Table 5.6). Based on the value of significance observed in Table 5.6, we conclude that guaranteed condition has no significant effect on users' risk-taking action compared to probable condition in the loss scenario. Hence, H3 is not supported.

Table 5.6. Results of Multinomial Logistic Regression Analysis for Expected Monetary Value of $100 in Loss Conditions

Download for $100[a]		B	Std. Error	Wald	df	Sig.	Exp(B)	95% Confidence Interval for Exp(B) Lower Bound	Upper Bound
1	Intercept	.208	.373	.309	1	.578			
	Loss [Monetary Polarity=0]	0[b]	.	.	0	.	.	.	.
	Guaranteed [Certainty=1]	.380	.543	.490	1	.484	1.463	.504	4.240
	Probable [Certainty=0]	0[b]	.	.	0	.	.	.	.

a. The reference category is: 0.

Table 5.7. Results of Multinomial Logistic Regression Analysis for Expected Monetary Value of $100 in Gain Conditions

Download for $100[a]		B	Std. Error	Wald	df	Sig.	Exp(B)	95% Confidence Interval for Exp(B) Lower Bound	Upper Bound
1	Intercept	-1.299	.461	7.958	1	.005			
	Gain [Monetary Polarity=1]	0[b]	.	.	0	.	.	.	.
	Probable [Certainty=0]	1.471	.572	6.613	1	.010	4.354	1.419	13.361
	Guaranteed [Certainty=1]	0[b]	.	.	0	.	.	.	.

a. The reference category is: 0.

From the results of the analysis as shown in the Table 5.7, we found that the variable Probable ($p = 0.010$) shows a significant effect in influencing the outcome to download the software application over the Guaranteed condition by 1.471 times in a Gain scenario, but the observed effect is in the opposite direction as H4. Hence, H4, which states that users are more willing to engage in risky computer security behavior in the guaranteed condition compared to the probable condition, H4 is not supported.

5.4. CHI-SQUARE ANALYSIS

The Chi-Square test is a statistical method that is used to measure the association between two or more categorical variables. The null hypothesis of the Chi-Square statistical test is that there is no existence of any relationship between the categorical variables in the total sample. The Chi-Square method is widely used by researchers to evaluate the Tests of Independence when using a crosstabulation. The crosstabulation method is also known as the bivariate table, as the variables tabulated and compared are categorical. The crosstabulation or crosstabs method is a tabular distribution of two categorical variables simultaneously, with the intersections of the categories of the variables appearing in the cells of the table. The Test of Independence measure assesses if there is any existing association between the variables by analyzing the pattern of the responses in the cells to the pattern that would be expected if the variables are truly independent of each other.

We use the Chi-Square statistical method to examine if there is an interaction between the independent variables (Monetary Polarity and the Certainty) on the user behavior (Download or Not Download) which is the response variable.

Table 5.8. Descriptive Statistics of Chi-Square Analysis

Monetary Polarity			Download or Not		
			Not Download	Download	Total
Loss	Certainty	Probable	18 (64.3%)	10 (35.7%)	28
		Guaranteed	16 (55.2%)	13 (44.8%)	29
	Total		34 (59.6%)	23 (40.3%)	57
Gain	Certainty	Probable	16 (45.7%)	19 (54.3%)	35
		Guaranteed	22 (78.6%)	6 (21.4%)	28
	Total		38 (60.3%)	25 (39.7%)	63
Total	Certainty	Probable	34 (54.0%)	29 (46.0%)	63
		Guaranteed	38 (66.7%)	19 (33.3%)	57
	Total		72 (60.0%)	48 (40.0%)	120

The descriptive statistics from the Chi-Square test shown in Table 5.8 indicate that 23 users (40.3% of those in loss scenario) chose to download the software to avoid a loss whereas 25 (39.7% of those in gain scenario) users chose to download to receive a gain.

The results of the Chi-Square statistical analysis (see Table 5.9) shows that for the Loss scenarios, value of chi-square statistic is 0.492 with 1 degree of freedom (df) and with a p-value of 0.483 (p-value > 0.05), which is not statistically significant. For the Gain scenarios, (see Table 5.9) the results of the chi-square tests show a value of 7.016 with 1 degree of freedom (df) and with a p-value of 0.08 (p-value > 0.05), which is also not statistically significant. These results show that there is no relationship between Certainty and User Download in both the Gain and Loss conditions.

Table 5.9. Results of Chi-Square Analysis

	Monetary Polarity	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Loss	Pearson Chi-Square	.492[c]	1	.483		
	Continuity Correction[b]	.186	1	.666		
	Likelihood Ratio	.493	1	.483		
	Fisher's Exact Test				.592	.334
	Linear-by-Linear Association	.483	1	.487		
	N of Valid Cases	57				
Gain	Pearson Chi-Square	7.016[d]	1	.008		
	Continuity Correction[b]	5.711	1	.017		
	Likelihood Ratio	7.275	1	.007		
	Fisher's Exact Test				.010	.008
	Linear-by-Linear Association	6.905	1	.009		
	N of Valid Cases	63				
Total	Pearson Chi-Square	2.011[a]	1	.156		
	Continuity Correction[b]	1.516	1	.218		
	Likelihood Ratio	2.021	1	.155		
	Fisher's Exact Test				.193	.109
	Linear-by-Linear Association	1.994	1	.158		
	N of Valid Cases	120				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 22.80.

b. Computed only for a 2x2 table

c. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 11.30.

d. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 11.11.

Based on the analysis, it is observed that the results from the linear regression statistical model and the chi-square statistical method are similar. We observe from the above results that the proposed hypothesis H1, H3 and H4 are not supported in both the cases. As chi-square is a descriptive test and not a modelling technique, and since we have explicitly defined a dependent variable (user behavior) for prediction, we consider the results from logistic regression model to be more appropriate for this study.

5.5. UNIVARIATE ANALYSIS OF VARIANCE FOR TIPPING POINT

The generalized linear model expands the general linear model such that there is a linear relation established between the dependent variable and the factors and covariates using a specific link function. The generalized linear model also allows the dependent variable to have a non-normal distribution. In the univariate analysis of variance (ANOVA), we compare the difference of the means between the groups. The factors or the groups in this method refer to the two independent variables used in the univariate analysis. The main objective of this model is to examine the relationship or an interaction between the factors and the dependent variable, i.e. between the two independent variables and the dependent variable. In the data analysis for our experimental study, we use the ANOVA to compare and analyze the tipping point (the Expected Monetary Value above which subjects choose to download the “Ad-Free Pro” application).

Since the maximum expected monetary value was set to $100 in the experiment, we were not able to analyze tipping points that were above $100 and hence, we removed all the data points with expected monetary value greater than $100 (i.e., we were not able to determine the tipping point for subjects who indicated that they would not download the

software in their first scenario that has an expected monetary value of $100). We removed these data points to avoid making any assumption about their tipping points (since they were above $100).

Table 5.10 provides the descriptive statistics for the dependent variables, tipping point, based on the independent variables, Monetary Polarity (Gain and Loss) and Certainty (Guaranteed and Probable). The variable N represents the number of subjects in a specific condition. The Mean value shown in Table 5.10 is the average tipping point value in every condition. Table 5.10 indicates that the mean tipping point of expected monetary value is $53.50 for the Probable Loss condition, $33.29 for the Probable Gain condition, $13.85 for the Guaranteed Loss condition, and $14.17 for the Guaranteed Gain condition.

Table 5.10. Descriptive Statistics of the Univariate Analysis of Variance

Dependent Variable: Tipping Point (TP)

Monetary Polarity	Certainty	Mean	Standard Deviation	N
Loss	Probable Loss	53.500	40.9980	10
	Guaranteed Loss	13.846	28.2034	13
	Total	31.087	39.0573	23
Gain	Probable Gain	33.289	37.5560	19
	Guaranteed Gain	14.167	11.5830	6
	Total	28.700	33.9893	25
Total	Probable	40.259	39.2755	29
	Guaranteed	13.947	23.8239	19
	Total	29.844	36.1307	48

Table 5.11 reports the results of the univariate ANOVA. The Sig column provides the p-value (2-tailed), which is used to assess if the effect by an independent variable or covariate is significant or not. In this case, we will compare each p-value to our preselected threshold for alpha value of 0.05. Coefficients having p-values less than this threshold for alpha value are statistically significant (Peng et al., 2002).

Table 5.11. Results of Tests of Between Subjects Effects for Tipping Point

Dependent Variable: Tipping Point (TP)

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	29108.395[a]	9	3234.266	3.811	.002
Intercept	4575.395	1	4575.395	5.392	.026
Importance of Primary Computer	1698.917	1	1698.917	2.002	.165
Threat Severity	88.549	1	88.549	.104	.748
Trust	10007.841	1	10007.841	11.793	.001
Fear	976.114	1	976.114	1.150	.290
Tolerance towards Ads	35.471	1	35.471	.042	.839
Cyber Security Awareness	216.999	1	216.999	.256	.616
Monetary Polarity	323.020	1	323.020	.381	.541
Certainty	5974.018	1	5974.018	7.040	.012
Monetary Polarity * Certainty	371.171	1	371.171	.437	.512
Error	32246.684	38	848.597		
Total	104106.250	48			
Corrected Total	61355.078	47			

a. R Squared = .474 (Adjusted R Squared = .350)

The p-value of the independent variable, Monetary Polarity, on dependent variable, tipping point, is not significant (p=0.541). However, the p-value of the independent variable, Certainty, on dependent variable, tipping point, is significant (p=0.012<0.05). Hence, Certainty has a main effect on the expected monetary value of the tipping point.

Among the covariates, Trust (T) shows a significant effect on the tipping point value, as it has a p-value (0.001<0.05). Other covariates such as Importance of Primary Computer (p-value = 0.165), Threat Severity (p-value = 0.748), Fear (p-value = 0.290), Tolerance towards Ads (p-value=0.839) and Cyber Security Awareness (p-value= 0.616) do not show any significant effect on the expected monetary value of the tipping point. Hence, all the covariates except Trust do not have a significant effect on the expected monetary value of the tipping point.

The results from the ANOVA also indicates that the p-value of the interaction is 0.512, and hence, there is no significant interaction of Monetary Polarity and Certainty on the expected monetary value of the tipping point. Although there is no significant interaction found, the independent variable, Certainty, has a significant main effect on the tipping point value.

Figure 5.1 illustrates the tipping values for all the four conditions involving Monetary Polarity and Certainty. Monetary polarity is represented on the horizontal axis and Certainty is plotted as two separate lines, one for the Guaranteed condition and the other for the Probable condition.

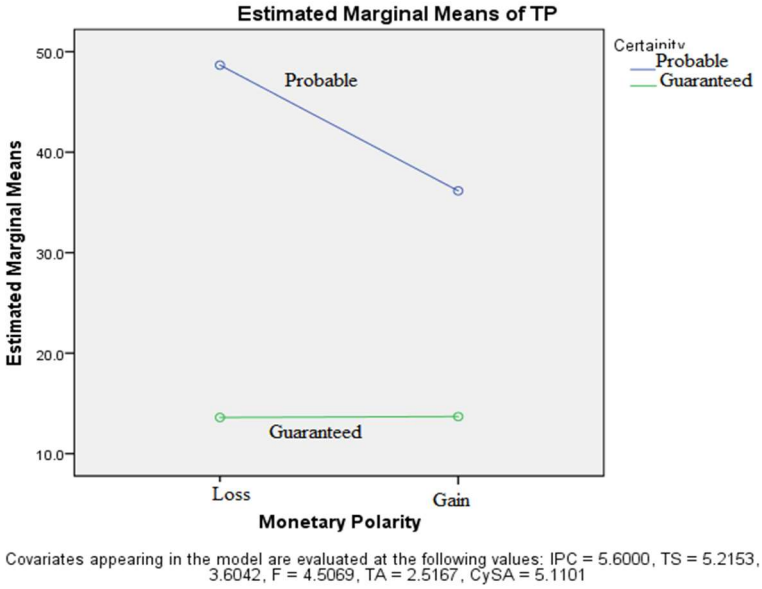


Figure 5.1. Interaction between Monetary Polarity and Certainty on Tipping Value

There is no significant interaction between Monetary Polarity and Certainty on the expected monetary value of the Tipping Point. Figure 5.1 shows that the Gain conditions do not have a higher tipping point of expected monetary value compared to the Loss conditions.

Based on the values from ANOVA, both the probable conditions (Probable Gain ($33.289) and Probable Loss ($53.500)) have higher expected monetary values of tipping points compared to the guaranteed conditions (Guaranteed Gain ($14.167) and Guaranteed Loss ($13.846)), which supports the finding that Certainty has a significant effect on the expected monetary value of the tipping point ($p=0.012<0.05$). Hence, H5 is supported.

Table 5.12 provides a summary of the results of hypothesis testing. H1-H4 are not supported and only H5 is supported. The next chapter discusses the findings.

Table 5.12. Results of Hypothesis Testing

Hypothesis	Supported?
H1: Users are more willing to engage in risky computer security behavior to avoid a loss than to receive a gain controlling for the amount net expected monetary value.	No
H2: Users exhibit a higher tipping point of expected monetary value to engage in risky computer security behavior when presented with a condition of experiencing gain compared to the condition of avoiding a loss.	No
H3: Users are more willing to engage in risky computer security behavior to avoid a guaranteed loss than a probable loss when the amount of expected loss is controlled.	No
H4: Users are more willing to engage in risky computer security behavior to receive a guaranteed gain than a probable gain when the amount of expected gain is controlled.	No
H5: Users exhibit a higher tipping point of expected monetary value to engage in risky computer security behavior when presented with a probable condition compared to a guaranteed condition in scenarios involving monetary gains or losses.	Yes

6. DISCUSSIONS

In line with prospect theory, the findings suggest that users in probable conditions will engage in risky cybersecurity activities at a higher tipping point of expected monetary value as compared to users in guaranteed conditions, regardless of whether it is a gain or loss scenario. In other words, users are more likely to engage in risky cybersecurity actions to receive a guaranteed gain or to avoid a guaranteed loss than to receive a probable gain or to avoid a probable loss when the amount of expected monetary value is controlled. Hence, providing a guaranteed gain or avoiding a guaranteed loss is more likely to lead users to take risky cybersecurity actions when compared to their equivalent probable conditions (i.e., that controlled for expected monetary values). In a gain scenario, users need to be rewarded with a higher value of expected monetary gain in a probable condition than a guaranteed condition in order to engage in risky cybersecurity behavior. Similarly, in a loss avoidance scenario, users expect a higher value of expected monetary loss avoidance in a probable condition than a guaranteed condition in order to engage in risky cybersecurity behavior.

Furthermore, the findings from our study also show that monetary polarity has no significant impact on users to partake a risky cyber security activity, while trust and cybersecurity awareness have a significant effect on users' decisions to take risky cybersecurity actions.

The results of the data analysis based on the hypotheses are summarized and discussed below:

First, there is no difference in users' risky computer security behavior when avoiding a loss or receiving a gain, which is not in line with prospect theory. We believe that human decision-making and behavior may be moderated by the way choices are presented to them. It is possible that prospect theory applies when individuals have to make a choice between different levels of risks or uncertainties but may not apply to accepting or rejecting a choice made under pre-determined scenarios of risks. Future research can explore this possibility in the application of prospect theory

Second, there is no difference in the tipping point of expected monetary value in the loss and gain conditions. Hence, the principle of loss aversion in prospect theory was not observed and people do not seem to value losses and gains differently when facing risky cybersecurity decisions.

Third, there is no difference in users' risky computer security behavior in a guaranteed and probable gain conditions. Similarly, there is also no difference in users' risky computer security behavior in a guaranteed and probable gain conditions.

Lastly, users are more willing to engage in risky computer security behavior at a higher tipping point of expected monetary value in the probable conditions compared to the guaranteed conditions in both gain and loss scenarios. The reason is that users prefer to receive a guaranteed gain or avoid a guaranteed loss as compared to their probable equivalent of expected value of the gain or loss. In line with prospect theory, a guaranteed gain is preferred to a probable gain with expected value controlled (risk aversion or certainty effect) and hence, the tipping point for guaranteed gains is lower than that for probable gains. Based on prospect theory, a probable loss is generally preferred to a guaranteed loss due to a preference for risk-seeking behavior when dealing with losses.

Hence, users are more interested to avoid a guaranteed loss as compared to avoiding a probable loss, with expected value being controlled. As such, the tipping point for avoiding a guaranteed loss is lower than the tipping point for avoiding a probable loss of the same expected value.

7. LIMITATIONS AND FUTURE RESEARCH

This research study had some limitations that can be resolved in the future research. To carry out the study in a controlled environment, the experiment was conducted in the computer labs of the Missouri University of Science and Technology, which we see as our first limitation. This was done to ensure that students were focused and not distracted by people or objects in the surrounding or environment. Hence, they could not use their laptop computers or their primary desktop computers to take part in the experiment. In future research, we would like subjects to participate in the experimental study using their primary personal computer or laptop. By using the above-mentioned procedure, we could analyze the cyber security behavior of users and their willingness to take risky cyber security actions on their primary personal computer or laptop.

Second, the experiment did not simulate any actual uncertified software download on the subjects' computers which could have made the experimental scenario more realistic. This can be overcome in future research by simulating an uncertified software download on the subjects' computers before presenting the experimental conditions.

Third, students who participated in the study mentioned in their suggestions that the number of conditions in the repeated measure of the experiment (i.e., varying expected monetary values) could be reduced. The subjects were presented with up to nine expected monetary value conditions based on their decisions to download the software from the uncertified developer to examine their tipping point for taking risky cyber security behavior. Future studies can overcome this limitation by increasing the starting value and the interval of the expected monetary value.

Lastly, we captured and analyzed very few perceptual outcomes such as Importance of Primary Computer, Threat Severity, Trust, Fear, Tolerance towards Ads, and Cyber Security Awareness as covariates. In future research, other covariates such as confidence of action of users, perceived severity, perceived risk, and other personality traits could be studied. The cybersecurity awareness measurement was more formative, than reflective, since they were based mostly on outcomes of cybersecurity actions and cybersecurity policies. Future studies can include more reflective measurement items for examining the cybersecurity awareness of users.

8. CONCLUSIONS

This research examines the impact of guaranteed and probable monetary gains and losses on the cybersecurity behavior of users using an experimental study. It also investigates the expected monetary value of the tipping point (minimum value for the user to take a risky cyber security action) of users in the guaranteed gain, probable gain, guaranteed loss, and probable loss conditions. It examines the effect of various user traits and perceptions, i.e., importance of primary computer, threat severity, trust, fear, tolerance towards ads, and cybersecurity awareness, as covariates in the study.

This study focuses on understanding the willingness of users to take risky cybersecurity actions to avoid a monetary loss as compared to receiving a monetary gain based on the prospect theory. The findings suggest that the loss condition does not affect users' software download decisions differently from the gain condition.

This research study also focuses on understanding the willingness of users to take risky cyber security actions when presented with guaranteed and probable monetary loss conditions. The findings suggest that the guaranteed loss and probable loss conditions have a similar effect on users' risky cybersecurity actions.

This research study also focuses on analyzing the willingness of users to take risky cyber security actions when presented with guaranteed and probable monetary gain conditions. The findings suggest that the guaranteed gains and probable gain conditions do not differ in their impact on the users' decision to take risky cyber security actions.

Based on the value function explained in the prospect theory, this experimental study focuses on examining whether users show a higher tipping point of expected

monetary value in the loss condition compared to the gain condition. It also focuses on understanding whether users show a higher expected monetary value of tipping point in the probable condition compared to the guaranteed condition in both gain and loss scenarios. The findings of this research suggest that the loss conditions do not have a significant effect on the expected monetary value of tipping point compared to the gain conditions. The findings also suggest that the probable conditions show a significant effect on users to have a higher expected monetary value of tipping point compared to the guaranteed conditions.

Moreover, the results of this study can help in predicting users' cybersecurity behavior based on guaranteed and probable monetary gains and losses. The results of this research provide an understanding about the tipping point of users which can be used to design effective spam filters to restrict phishing emails and other cybersecurity threats. The findings from this research study can also be used to warn and train employees about avoiding phishing emails and thereby preventing employees from taking risky cyber security actions for monetary gains and losses.

APPENDIX A

SCENARIO DETAILS

MISSOURI S&T

SCENARIO

You have been experiencing **a lot of ads on your primary computer** recently and need to install an ad blocker software on your primary computer.

You have received **$200 free credits in your Amazon shopping account** (that you can use to buy anything at Amazon.com) for subscribing to a promotion email list from an **uncertified developer** and that **uncertified developer** is now offering an **Ad-Free Pro software that provides an Ad free browsing experience** that **no software** in the market can provide.

APPENDIX B

EXPERIMENTAL CONDITIONS

SCENARIO 1: GUARANTEED GAIN

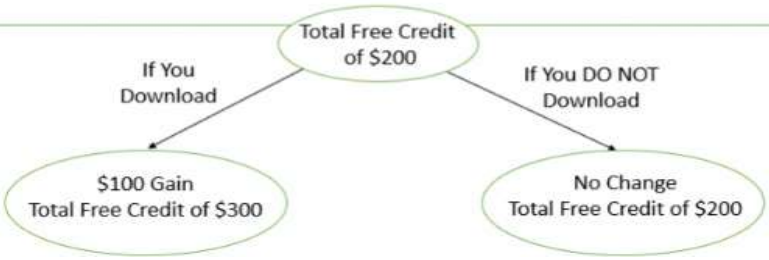
1.1. Guaranteed Gain with $100 Expected Monetary Value

FIRST SCENARIO: You now have **$200 free credits in your Amazon shopping account**.

Will you download "Ad-Free Pro" from the **Uncertified Developer** on your primary **computer** based on the following conditions?

CONDITIONS FOR DOWNLOAD FROM THE UNCERTIFIED DEVELOPER:

1. If you **DOWNLOAD** "Ad-Free Pro", you will receive $100 free credit in your Amazon shopping account, resulting in a total free credit of $300.
2. If you **DO NOT DOWNLOAD** "Ad-Free Pro", the free credit in your Amazon shopping account remains unchanged, resulting in a total free credit of $200.



Please answer the following question about the scenario:

If you choose to download the "Ad-Free Pro" software, you will gain $_____

Please justify your rationale for choosing to **Download or Not Download**:

Given the above conditions, do you want to download "Ad-Free Pro"?

Yes | No

SCENARIO 2: GUARANTEED LOSS

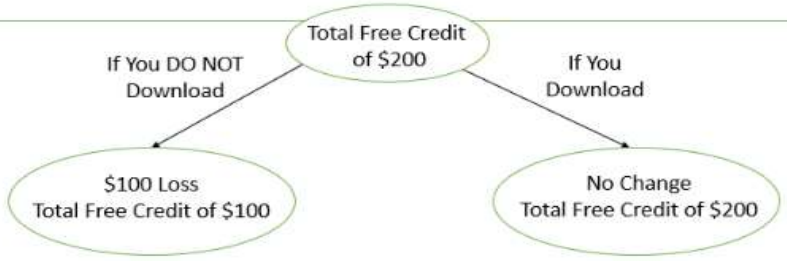
2.1 Guaranteed Loss with $100 Expected Monetary Value

FIRST SCENARIO: You now have **$200 free credits in your Amazon shopping account**.

Will you download "Ad-Free Pro" from the **Uncertified Developer** on your primary **computer** based on the following conditions?

CONDITIONS FOR DOWNLOAD FROM THE UNCERTIFIED DEVELOPER:

1. If you **DO NOT DOWNLOAD** "Ad-Free Pro", you will lose $100 free credits in your Amazon shopping account, resulting in a total free credit of $100.
2. If you **DOWNLOAD** "Ad-Free Pro", the free credit in your Amazon shopping account remains unchanged, resulting in a total free credit of $200.



Please answer the following question about the scenario:

If you choose NOT to download the "Ad-Free Pro" software, you will lose $_____

Please justify your rationale for choosing to **Download or Not Download**:

Given the above conditions, do you want to download "Ad-Free Pro"?

Yes | No

SCENARIO 3: PROBABLE GAIN

3.1. Probable Gain with $200 Expected Monetary Value

FIRST SCENARIO: You now have **$200 free credits in your Amazon shopping account**.

Will you download "Ad-Free Pro" from the **Uncertified Developer** on your primary **computer** based on the following conditions?

CONDITIONS FOR DOWNLOAD FROM THE UNCERTIFIED DEVELOPER:

1. If you **DOWNLOAD** "Ad-Free Pro", there is a 50% chance that you receive $200 free credits in your Amazon shopping account, resulting in a total free credit of $400.
2. If you **DO NOT DOWNLOAD** "Ad-Free Pro", the free credit in your Amazon shopping account remains unchanged, with a total free credit of $200.

Please answer the following question about the scenario:

If you choose to download the "Ad-Free Pro" software, there is a 50% chance you will gain $_____

Please justify your rationale for choosing to **Download or Not Download**:

Given the above conditions, do you want to download "Ad-Free Pro"?

Yes | No

SCENARIO 4: PROBABLE LOSS

4.1. Probable Loss with $200 Expected Monetary Value

FIRST SCENARIO: You now have **$200 free credits in your Amazon shopping account**.

Will you download "Ad-Free Pro" from the **Uncertified Developer** on your primary **computer** based on the following conditions?

CONDITIONS FOR DOWNLOAD FROM THE UNCERTIFIED DEVELOPER:

1. If you **DO NOT DOWNLOAD** "Ad-Free Pro", there is a 50% chance that you lose $200 free credits in your Amazon shopping account, resulting in a total free credit of $0.

2. If you **DOWNLOAD** "Ad-Free Pro", the free credit in your Amazon shopping Account remains unchanged, resulting in a total free credit of $200.

Please answer the following question about the scenario:

If you choose NOT to download the "Ad-Free Pro" software, there is a 50% chance you will lose $_____

Please justify your rationale for choosing to **Download or Not Download**:

Given the above conditions, do you want to download "Ad-Free Pro"?

Yes | No

APPENDIX C

MANIPULATION CHECK QUESTIONS

1. Gain Conditions (In both Guaranteed and Probable)

   1.1. In the scenarios above, on downloading the "Ad-Free Pro" software, you experience a _____.

   1.2.In the scenarios above, on downloading the software, what are your chances of experiencing a gain/loss?

2. Loss Conditions (In both Guaranteed and Probable)

   a. In the scenarios above, on not downloading the "Ad-Free Pro" software, you experience a _____.

   b. In the scenarios above, on not downloading the software, what are your chances of experiencing a gain/loss?

APPENDIX D

CONTROL CONDITION

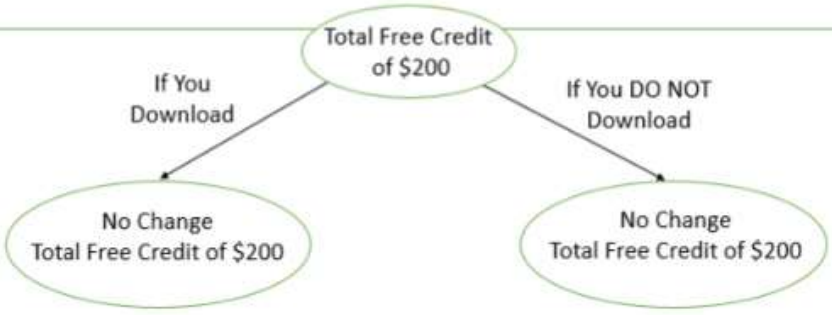
1. **Guaranteed Gain**

NEW SCENARIO: You now have **$200 free credits in your Amazon shopping account**.

Will you download "Ad-Free Pro" from the **Uncertified Developer** on your primary **computer** based on the following conditions?

CONDITIONS FOR DOWNLOAD FROM THE UNCERTIFIED DEVELOPER:

1. If you **DOWNLOAD** "Ad-Free Pro", the free credit in your Amazon shopping account remains unchanged, resulting in a total free credit of $200.
2. If you **DO NOT DOWNLOAD** "Ad-Free Pro", the free credit in your Amazon shopping account remains unchanged, resulting in a total free credit of $200.



Please answer the following question about the scenario:

If you choose to download the "Ad-Free Pro" software, you will gain $____

Please justify your rationale for choosing to **Download or Not Download**:

Given the above conditions, do you want to download "Ad-Free Pro"?

Yes | No

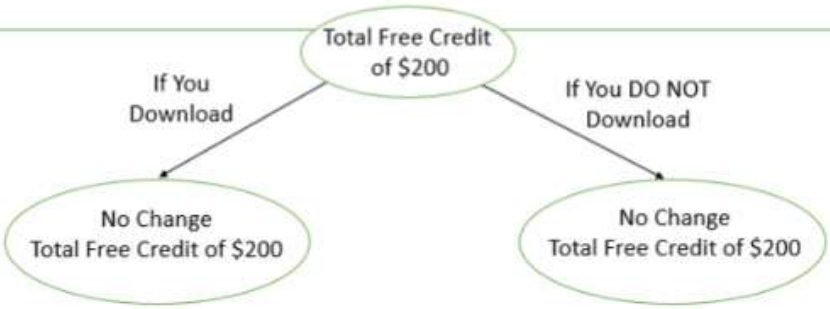
2. Guaranteed Loss

NEW SCENARIO: You now have **$200 free credits in your Amazon shopping account**.

Will you download "Ad-Free Pro" from the **Uncertified Developer** **on your primary computer** based on the following conditions?

CONDITIONS FOR DOWNLOAD FROM THE UNCERTIFIED DEVELOPER:

1. If you **DOWNLOAD** "Ad-Free Pro", the free credit in your Amazon shopping account remains unchanged, resulting in a total free credit of $200.
2. If you **DO NOT DOWNLOAD** "Ad-Free Pro", the free credit in your Amazon shopping account remains unchanged, resulting in a total free credit of $200.



Please answer the following question about the scenario:

If you choose to download the "Ad-Free Pro" software, you will lose $____

Please justify your rationale for choosing to **Download or Not Download**:

Given the above conditions, do you want to download "Ad-Free Pro"?

Yes | No

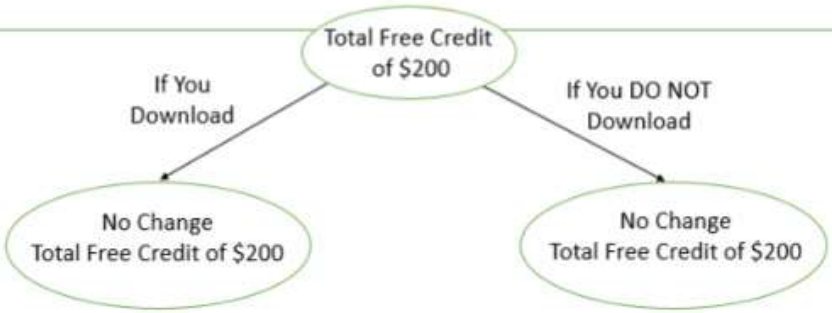
3. Probable Gain

NEW SCENARIO: You now have **$200 free credits in your Amazon shopping account**.

Will you download "Ad-Free Pro" from the **Uncertified Developer** on your primary **computer** based on the following conditions?

CONDITIONS FOR DOWNLOAD FROM THE UNCERTIFIED DEVELOPER:

1. If you **DOWNLOAD** "Ad-Free Pro", the free credit in your Amazon shopping account remains unchanged, resulting in a total free credit of $200.
2. If you **DO NOT DOWNLOAD** "Ad-Free Pro", the free credit in your Amazon shopping account remains unchanged, resulting in a total free credit of $200.



Please answer the following question about the scenario:

If you choose to download the "Ad-Free Pro" software, you will gain $____

Please justify your rationale for choosing to **Download or Not Download**:

Given the above conditions, do you want to download "Ad-Free Pro"?

Yes | No

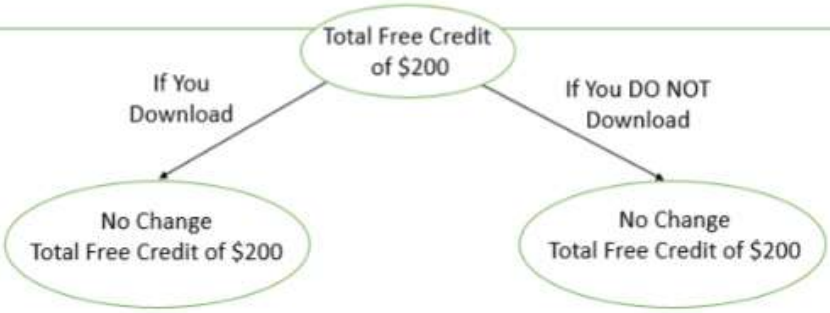
4. Probable Loss

NEW SCENARIO: You now have **$200 free credits in your Amazon shopping account**.

Will you download "Ad-Free Pro" from the **Uncertified Developer** on your primary **computer** based on the following conditions?

CONDITIONS FOR DOWNLOAD FROM THE UNCERTIFIED DEVELOPER:

1. If you **DOWNLOAD** "Ad-Free Pro", the free credit in your Amazon shopping account remains unchanged, resulting in a total free credit of $200.
2. If you **DO NOT DOWNLOAD** "Ad-Free Pro", the free credit in your Amazon shopping account remains unchanged, resulting in a total free credit of $200.



Please answer the following question about the scenario:

If you choose to download the "Ad-Free Pro" software, you will lose $____

Please justify your rationale for choosing to **Download or Not Download**:

Given the above conditions, do you want to download "Ad-Free Pro"?

Yes | No

APPENDIX E

QUESTIONNAIRE TO ASSESS PERCEPTUAL OUTCOMES

Measurement of Perceptual Outcomes

	Measurement Items
Importance of Primary Computer (IPC)	(IPC1) I have important files stored on my primary computer.
	(IPC2) My primary computer is valuable to me.
	(IPC3) The data on my primary computer is important to me.
	(IPC4) I cannot afford to lose the files on my primary computer.
	(IPC5) I will not risk the security of my primary computer.
	(IPC6) My primary computer is very important to me.
Threat Severity (TS) (Johnston & Warkentin, 2010)	(TS1) If my computer were infected by malware because of downloading the "Ad-Free Pro" application, it would be severe.
	(TS2) If my computer were infected by malware because of downloading the "Ad-Free Pro" application, it would be serious.
	(TS3) If my computer were infected by malware because of downloading the "Ad-Free Pro" application, it would be significant.
Trust (T) (Freed, 2014)	(T1) I believe the "Ad-Free Pro" application is a trustworthy application.
	(T2) I trust the vendor of the "Ad-Free Pro" application.
	(T3) I trust the "Ad-Free Pro" application.

Fear (F) (Freed, 2014)	(F1) I was worried about downloading the "Ad-Free Pro" application.
	(F2) I was concerned about downloading the "Ad-Free Pro" application.
	(F3) I experienced fear when deciding if I should download the "Ad-Free Pro" application.
Tolerance towards Ads (TA)	(TA1) I hate having ads on my primary computer.
	(TA2) Having ads on my primary computer is fine with me.
	(TA3) I am bothered by ads on my primary computer.
	(TA4) I like to have ads on my primary computer.
	(TA5) I do not mind having ads on my primary computer.
	(TA6) I do not want ads on my primary computer.

APPENDIX F

QUESTIONNAIRE TO ASSESS DEMOGRAPHICS INFORMATION

1. Gender - What is your gender? (Male, Female)
2. Age - How old are you? (18-24, 25-34, 35-44, 45-54, 55-64, 65-74 and, 75 or older)
3. Please specify your ethnicity. (White, Black or African American, American Indian or Alaska Native, Asian, Native Hawaiian or Pacific Islander, Hispanic or Latino, Other, Prefer Not to Disclose)
4. What is your marital status? (Single, Married, Widowed, Divorced, Separated)
5. How many hours do you spend online per week approximately? (1-5, 6-10, 11-15, 16-20, 20+)
6. How often do you download software from the internet? (Rarely or Never, Once a Month, Two or Three Times a Month, Four or More Than Four Times a Month)
7. What is your major field of study? (Information Science & Technology, Business Management, Engineering, Pyschology, Other)
8. Are you an undergraduate student, graduate student or a certificate-seeking (only) student? (Undergraduate Student, Graduate Student, Certificate-Seeking, Other)
9. What statement best describes your current employment status? (Working (Paid Employee), Working (Self-employed), Not Working, Prefer Not to Disclose)
10. Please indicate the answer that includes your entire family income in (previous year) before taxes. (Less than $10,000, $10,000 to $49,999, $50,000 to $99,999, $100,000 to $149,999, $150,000 or more)
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)

APPENDIX G

QUESTIONNAIRE TO ASSESS USERS' CYBERSECURITY AWARENESS

1. I am careful when downloading third-party software.
2. I often download from third party websites.
3. My computer often gets infected by viruses.
4. I do not use anti-virus software on my computer.
5. I frequently update the anti-virus software on my computer.
6. I have anti-virus software installed, updated, and enabled on my computer.
7. I often download and install unlicensed software.

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.

Anderson, C & Agarwal . (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. MIS Quarterly, 16(3), 613-643.

Aurigemma, S. & Panko, R. R. (2010) The detection of human spreadsheet errors by humans versus inspection (auditing) software, Proceedings of the European Spreadsheets Risks Interest Group, University of Greenwich, London, 73-85.

Beebe, N. L., Young, D. K., & Cheng, F. R. (2014) Framing information security budget requests to influence investment decisions, Communications of the Association for Information Systems, 35(7), 133-143.

Block, L. G., & Keller, P. N. (1995). When to accentuate the negative: The effects of perceived efficacy and message framing on intentions to perform health-related behavior. Journal of Marketing Research, 32, 192-204.

Brewer, M. B., & Kramer, R. M. (1986). Choice behavior in social dilemmas: Effects of social identity, group size, and decision framing. Journal of Personality and Social Psychology, 50(3), 543-549.

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

Chan, H. A., & Mubarak, S. (2012). Significance of information security awareness in the higher education sector. International Journal of Computer Applications, 60(10), 23-31.

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

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

D'Arcy, J. H. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79-98,155,157.

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

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

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

Farahmand, F., & Spafford, E. H.. (2013). Understanding insiders: An analysis of risk-taking behavior. Information Systems Frontiers, 15(1), 5-15.

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

Fishburn, P. C. (1970). Utility theory for decision making (No. RAC-R-105). Research Analysis Corp., Mclean, VA.

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

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

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

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

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

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

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

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

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

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

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

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

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

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' information security awareness and behavior: A literature review. Proceedings of the 46th Hawaii International Conference on System Sciences (pp. 2978 - 2987). Wailea, HI: IEEE Computer Society.

Lee, A. Y., & Aaker, J. L. (2004). Bringing the frame into focus: The influence of regulatory fit on processing fluency and persuasion. Journal of Personality and Social Psychology, 86(2), 205-218.

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

Liang, H. a. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11, 7, 394-413.

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

Manjak, M. (2006). Social Engineering Your Employees to Information Security[PDF]. GIAC Gold Paper for Security Essentials, 16-17.

McDermott, R. (1991). Risk-Taking in International Politics. The University of Michigan Press: Ann Arbor, MI.

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

Nah, F. C. (2017). Impact of monetary value gains and losses on computer security behavior of users. Proceedings of IFIP WG8.11/WG11.13 2017 Dewald Roode Workshop on Information Systems Security Research, Tampa, Florida.

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

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

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. Proceedings of the 40th Annual Hawaii International Conference on System Sciences. IEEE Computer Society.

Panko, R. R. (2010). Revising the Panko–Halverson taxonomy of spreadsheet errors. Decision Support Systems, , 49(2), 235-244.

Pechmann, C., Zhao, G., Goldberg, M., & Reibling, E. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. Journal of Marketing, 67(2), 1-18.

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

Plous, S. (1993). The Psychology of Judgment and Decision Making. McGraw-Hill Education.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93-114.

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

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122-131.

Shiv, B., Edell, J., & Payne, J. W. (2004). Does elaboration increase or decrease the effectiveness of negatively versus positively framed messages? Journal of Consumer Research, 31(1), 199-208.

Shoshitaishvili, Y., Invernizzi, L., Doupe, A., & Vigna, G. (2014). Do you feel lucky? A large-scale analysis of risk-rewards trade-offs in cyber security. Proceedings of the ACM Symposium on Applied Computing, Association for Computing Machinery, 1649-1656.

Siponen, M. T. (2000a). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31-41.

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

Smith, S. N. (2017). The impact of monetary value gains and losses on cybersecurity behavior. Proceedings of the Midwest Association for Information Systems Conference, Springfield, Illinois.

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, NY.

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

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

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

Tversky, A., & Kahneman, D. (1986). Rational choice and the framing of decisions. The Journal of Business, 59(4), S251-S278.

Tyler, T. R. (2005). Can businesses effectively regulate employee conduct? Academy of Management Journal, 48, 6, 1143-1158.

Vardi, Y., & Weitz, E. (2003). Misbehavior in organizations: Theory, research, and management. Misbehavior in organizations: Theory, research, and management, 1-337.

Valecha, R. C. (2016). Reward-based and risk-based persuasion in phishing emails. Proceedings of the 2016 IFIP WG8.11/WG11.13 Dewald Roode Workshop on Information Systems Security Research.

Verendel, V. (2009). Quantified security is a weak hypothesis: A critical survey of results and assumptions. Paper presented at the Proceedings New Security Paradigms Workshop, 37-49.

Warkentin, M. & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. European Journal of Information Systems, 18, 2, 101-105.

Weitz, Y. V. (2004). Misbehavior in Organizations: Theory, Research, and Management. Mahwah, NJ: Lawrence Erlbaum Associates. Lawrence Erlbaum Associates, 337.

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

Witte, K. (1992). Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model. Communication Monographs, 59, 329-349.

Witte, K. C. (1996). Predicting risk behaviors: Development and validation of diagnostic scale. Journal of Health Communication 1, 317-341.

Woon, I., Tan, G.-W., & Low, R. T. (2005). A protection motivation theory approach to home wireless security. Proceedings of the 26th International Conference on Information Systems, (pp. 367-380). Las Vegas, NV.

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

VITA

Santhosh Kumar Ravindran was born in Chennai, Tamil Nadu, India. In June 2014, he received his Bachelor's degree in Information Science and Technology from Anna University, Chennai, Tamil Nadu, India. He worked as an iOS Software Engineer at Zoho Corporation, India from June 2014 – July 2016. He then joined Missouri University of Science and Technology (formerly known as University of Missouri – Rolla) in Fall 2016. He earned a Graduate Certificate in Business Analytics and Data Science in December 2017. In July 2018, he received his M.S in Information Science and Technology from Missouri University of Science and Technology. During the course of his Master's degree, he pursued an internship with The Boeing Company, where he worked as a Software Developer Intern in 2017.