2021

The Empirical Study of the Factors that Influence Threat Avoidance Behavior in Ransomware Security Incidents

Heriberto Aurelio Acosta Maestre

The Empirical Study of the Factors that Influence Threat Avoidance Behavior in Ransomware Security Incidents

by

Heriberto A. Acosta-Maestre

A Dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Computing and Engineering
Nova Southeastern University
2021

We hereby certify that this dissertation, submitted by Heriberto A. Acosta conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

11/25/21

Inkyoung Hur, Ph.D. **Date**
Chairperson of Dissertation Committee

11/25/21

Ling Wang, Ph.D. **Date**
Dissertation Committee Member

Souren Paul

11/25/21

Souren Paul, Ph.D. **Date**
Dissertation Committee Member

Approved:

11/25/21

Meline Kevorkian, Ed.D. **Date**
Dean, College of Computing and Engineering

College of Computing and Engineering
Nova Southeastern University

2021

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

The Empirical Study of the Factors that Influence Threat Avoidance Behavior in Ransomware Security Incidents

By
Heriberto A. Acosta-Maestre
October 2021

Ransomware security incidents have become one of the biggest threats to general computer users who are oblivious to the ease of infection, severity, and cost of the damage it causes. University networks and their students are susceptible to ransomware security incidents. College students have vast technical skills and knowledge, however they risk ransomware security incidents because of their lack of mitigating actions to the threats and the belief that it would not happen to them. Interaction with peers may play a part in college students’ perception of the threats and behavior to secure their computers. Identifying what influences students’ threat avoidance behavior in the face of ransomware security incidents is essential to managing students’ behaviors to protect their personal and university computer systems. The goal of this research is to empirically examine threat avoidance behavior in the context of ransomware security incidents among college students. The research model extends the Technology Threat Avoidance Theory with the addition of the factors of subjective norm, attitude toward knowledge sharing, and experience of threat. The study focuses on the effects these factors have on threat avoidance behavior. These factors determine if externalities such as social pressures or previous experiences of threat influence avoidance behavior.

This study was a quantitative and empirical study using a non-probability design for gathering data. The convenience sampling method was used to collect data using a survey instrument. The items of the survey instrument were designed using the 7-point Likert Scale. The data was collected from 174 United States college students using an online survey tool. Prior to the main data collection effort, an expert panel review and a pilot study were conducted. Pre-analysis data screening was conducted before analyzing the data. Data analysis with survey data was conducted using Partial Least Square Structural Equation Modeling (PLS-SEM) using SmartPLS 3.0.

The results of the study showed a positive and significant relationship between avoidance motivation and threat avoidance behavior. Subjective norm was found to have a positive effect on attitude towards knowledge sharing. However, the relationship between subjective norm and response efficacy was not significant. The study contributes to the body of knowledge by providing empirical evidence about the effect of factors of threat avoidance behavior on ransomware security incidents among college students. It provides insight into the experience and preparedness of students to deal with the threat of ransomware.

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background / Introduction

According to Fimin (2017), in 2016 half of all the companies in the United States had their systems infected by a type of ransomware with many of them paying the hackers an average ransom of $2,500. The author also pointed to a Federal Bureau of Investigation (FBI) study that calculated the total cost of these ransoms at $1 billion during 2016.

Yan et al. (2018) argue that students have unsafe computer behaviors; students tend to trust most communications such as emails as long as they came from close friends. Yan et al. (2018) also found that even students with computer security knowledge and skills would choose to ignore good security practices.

Stanciu and Tinca (2016) demonstrated that students falsely believed they had above average computer security knowledge. However, Scheponik et al. (2016) found that students lack the skills and knowledge to protect their computers from security threats. Students in the study felt comfortable with the level of safety provided by the most basic of computer security solutions. For example, some students felt secure using encryption alone and did not understand that good security requires multiple tools and methods. The students also had difficulty understanding the difference between authentication and authorization. According to Zhang-Kennedy et al. (2018), students from a university affected by ransomware felt there was nothing they could do to protect themselves against such an attack and were indifferent towards increasing their cybersecurity skills and knowledge.

Problem Statement

Ransomware has grown exponentially since Dr. Joseph Popp created and distributed the first ransomware in 1989 (Nadir & Bakhshi, 2018). According to O'Gorman et al. (2019), they detected nearly 545,000 ransomware attacks in 2018; 81% of which affected enterprise users. Ransomware has become more sophisticated, harder to detect, and easier to spread in a local network (O'Gorman et al., 2019). Sultan, Khalique, Alam, and Tanweer (2018) state that from 2015 to 2016, the United States was the target of 28% of all ransomware attacks and more than 50% of affected users were consumers. The authors also mention that during 2016, the average affected user paid $1,000 to recover their files.

Zhang-Kennedy et al. (2018) found that students of ransomware affected universities were worried about cybersecurity shortly after the attack and some even began taking concrete steps to have recent backups; a peak of 78% of students began making data backups. However, as time passed, cybersecurity concerns decreased. In addition, 57% of the students thought the university could have prevented the ransomware attack. These same students decided to ignore cybersecurity education material because they felt there was little they could do to protect their systems against ransomware.

This study examined the effect of the knowledge sharing attitude of college students regarding the threat of ransomware security incidents. It is important to know if college students share security incident experiences with each other as this organic exchange of knowledge may protect the group more efficiently.

The accumulation of firsthand knowledge, also known as experience, is of utmost importance when facing a threat (Venkatesh, Brown, Maruping, & Bala, 2008). Experience of threat is not necessarily a given; especially among risk prone students who believe they are invincible (van Schaik et al., 2017). It is important to understand how the experience of threat affects threat avoidance behavior.

Liang and Xue investigated the relationships around threat avoidance behavior. Liang and Xue (2009) created the Technology Threat Avoidance Theory (TTAT), while the study of Liang and Xue (2010) validated the TTAT and tried to understand how it works. Liang and Xue (2010)'s study was done with a small group of college students. The authors also mention that the sources of threats and safeguards can be changed, while also suggesting the effect of emotion in the model. The TTAT is a very flexible framework. Liang and Xue (2010) state that it can be used to study several threats and mitigating actions. They recommend that future research could be done with coping based mitigating actions.

Ng and Rahim (2005) studied the home user's intention to practice computer security. Building their study on the Theory of Planned Behavior (TPB), one of the factors they focused on was the subjective norm. Their study concluded that subjective norm did in fact play a part in the user's decision to practice computer security. Chi, Yeh, and Hung (2012) studied the effect of subjective norm on a user's perceived risk and usage intention towards cloud computing services. They found that the influence of subjective norm on usage intention is greater than the influence of perceived risk.

Attitude toward knowledge sharing is important in a group facing a threat and is derived from the attitude in the TPB (Ajzen, 1991). Zhang, Tsang, Yue, and Chau (2015) argue there are similarities in how computer security experts and general topic online learning communities share information amongst themselves. The authors observed that those who are inexperienced remain as observers, while expert hackers share more knowledge and advice with inexperienced hackers. Also, less experienced hackers tend to ask questions and share more about their experience in search of guidance. The authors conclude that even in the anarchical world of hackers, online communities have a structure like any other merit-based learning community.

The volatile mix of modern ransomware and the apparent ignorance or indifference from college students is dangerous to college networks (Zhang-Kennedy et al., 2018). The study tests the relationship among the factors affecting threat avoidance behavior on ransomware security incidents among college students. College students have vast technical skills and knowledge. However, they risk ransomware security incidents because of their lack of mitigating actions to the threats and the belief that it will not happen to them. The peculiarities of young adults and their risk prone behavior pose a risk to their personal systems and their university’s networks. We currently do not know the factors influencing college students’ security behavior involving interaction with peers. How college students’ threat avoidance behavior is influenced, and by which factors, needs to be studied to understand how to mitigate the risks. Research into Information Technology (IT) threat avoidance behavior has mostly focused on enterprise and business users leaving a large gap in the general user population.

Dissertation Goal

The research goal was to empirically examine a research model of threat avoidance behavior in the context of ransomware security incidents among college students. The model extended the TTAT by Liang and Xue (2010) with three additional factors - subjective norm, attitude toward knowledge sharing, and experience of threat - and focused on the effect these factors have on IT threat avoidance behaviors in ransomware security incidents.

Research Questions

1. How does subjective norm affect the attitude toward knowledge sharing among peers following a ransomware security incident?
2. How does the experience of threat affect the perceived threat when a user discovers a peer has been infected by ransomware?
3. How does attitude toward knowledge sharing affect perceived susceptibility threat following a ransomware security incident?
4. How does subjective norm affect a user’s response efficacy following a ransomware security incident?
5. How does perceived threat affect a user’s avoidance motivation following a ransomware security incident?
6. How does coping appraisal affect a user’s avoidance motivation following a ransomware security incident?
7. How does avoidance motivation affect a user’s threat avoidance behavior following a ransomware security incident?

Research Model

The research empirically examined a research model of threat avoidance behavior. The research model shown in Figure 1, represents factors that influence threat avoidance behavior and variables used to test the hypothesis.

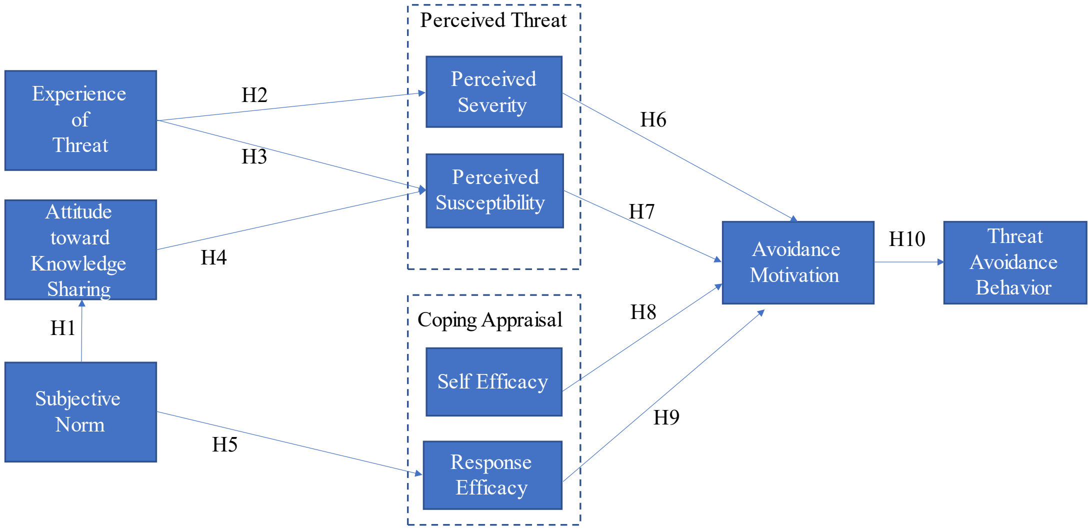


Figure 1. Research model of Threat Avoidance Behavior

Subjective norm has a positive effect on attitude toward knowledge sharing as the greater subjective norms lead to greater sharing (Tu, Turel, Yuan, & Archer, 2015). Bock, Zmud, Kim, and Lee (2005) also found that subjective norms had a positive effect on the attitude toward knowledge sharing. There is also a positive attitude toward information sharing if there is a subjective norm among the immediate social group, which will encourage a greater exchange of information among the individuals (Jarvenpaa & Staples, 2000). Therefore, the following hypothesis is developed:

H1: Subjective Norm has a positive effect on Attitude toward Knowledge Sharing.

The construct experience of threat is positively associated with perceived susceptibility and perceived severity, since having experience with a threat increases the user’s perception that the threat can happen again to a greater degree than the first time. Individuals who go through a negative experience have a higher probability of being hypervigilant to that vulnerability in future situations (Tu et al., 2015). Therefore, the following hypothesis is developed:

H2: Experience of Threat has a positive effect on Perceived Severity.

H3: Experience of Threat has a positive effect on Perceived Susceptibility.

Attitude toward knowledge sharing is positively associated with perceived susceptibility as more shared information about threats possibly increase the user’s perceptions that something can happen (Bock et al., 2005). This construct captures how willing an individual is to share their knowledge with others. Therefore, the following hypothesis is developed:

H4: Attitude toward Knowledge Sharing has a positive effect on Perceived Susceptibility.

Social influence or pressure has been shown to affect the threat avoidance behavior of information system users as people function most of the time as part of social units (Liang & Xue, 2009). Humans are social animals, and their behavior would be constantly affected by the actions and beliefs of other humans. The authors observed that most users would eventually fall in line and conform to behaviors that are acceptable to the rest of their social group. Social influences not only pressure users into behaving in one way or another but also provide them with valuable information about what is acceptable by their current group (Liang & Xue, 2009). This information may help the user predict the risks of the possible IS threat and how viable the available mitigating actions or tools are.

Taylor and Todd (1995) argue that behavioral intentions are highly likely to be preceded by subjective norms.

The construct subjective norm has a larger effect when the individual has little experience and has yet to adopt a certain attitude (Chua, 1980). Subjective norm is a determinant of intention and has an indirect but significant effect on behavior (Taylor & Todd, 1995). Also, Tu et al. (2015) argue that social influences directly influence an individual's coping intentions. By increasing the individual's threat perceptions, subjective norms push them to find way to mitigate the perceived threat (Tu et al., 2015). Chi et al. (2012) argue that subjective norm has a greater influence on individuals that perceived risk. Individuals yield to society and group pressures to use a system even if they perceive that system to be at risk. Individuals, for the most part, follow the observed behavior of their immediate environment and group (Chan, Woon, & Kankanhalli, 2005). Since subjective norm affects an individual's behavior, there should be a relationship with how said individual reacts or behaves when facing the threat of ransomware. Therefore, the following hypothesis is developed:

H5: Subjective Norm has a positive effect on Response Efficacy.

As per the model by (Liang & Xue, 2010), the constructs of coping appraisal and perceived threat have a positive association with avoidance motivation to threat avoidance behavior. (Liang & Xue, 2010) empirically proved that individuals would be motivated to avoid a threat if they have an elevated level of self-efficacy. Also, they found that avoidance motivation has a significant influence on threat avoidance behavior. Therefore, the following hypothesis is developed:

H6: Perceived Severity has a positive effect on Avoidance Motivation.

H7: Perceived Susceptibility has a positive effect on Avoidance Motivation.

H8: Self-Efficacy has a positive effect on Avoidance Motivation.

H9: Response Efficacy has a positive effect on Avoidance Motivation.

H10: Avoidance Motivation has a positive effect on Threat Avoidance Behavior.

Relevance and Significance

The results of the research contribute to the body of knowledge by providing empirical evidence about the effect of factors of threat avoidance behavior on ransomware security incidents among college students.

Scheponik et al. (2016) argue that students are an important threat vector. The authors point out that a significant number of college students, either by ignorance or over-confidence, do not have the technical knowledge to understand basic security topics. The adage that students cannot see the forest for the trees holds true with students as they are not able to see the big picture of the threat posed by ransomware. Most students feel confident with only one threat mitigation solution (Scheponik et al., 2016).

Stanciu and Tinca (2016) stated that universities are concerned with the lack of risk awareness shown by a significant number of students. Universities are becoming aware of the security risks that companies face today and are interested in creating curriculums and preparing future professionals that have basic security knowledge. The study by (Stanciu & Tinca, 2016) also revealed that almost 3/4th of the students surveyed know of a friend that has had a security breach. However, even with the knowledge that a friend or a colleague had a breach, half of the students responded that they did not think their computers would be targeted by hackers. A large majority of these same students believe that having an antivirus is not enough protection. However, that same group uses only an antivirus for computer threat protection.

The study provides greater practical insight into how college students are reacting to ever more common ransomware-based security threats. This new information helps universities know where and how to better focus their risk awareness training. This effort should trickle down the workforce into the industry as security-aware students become professionals that understand the risks and have the right motivations to follow the security policies in their workplaces.

Also, the TTAT is a flexible and reliable framework. However, there is not a lot of scientific literature using the TTAT to study student threat avoidance behavior as most studies tend to focus on company employees. Also, extending the TTAT with constructs that focus on social connections and interactions adds the component of human interconnectivity that has been modifying our behavior since the start of the social media age. This hyper connected age we live in, where we are not just influenced by our next-door neighbor but by friends a world apart brings new variables that are interesting to study. Before social media, college students would have known only of the ransomware breach of their roommate but in today’s world, they will find out about dozens or hundreds of breaches around their local campus or friends in other campuses of their school system.

Barriers and Issues

This study used a survey instrument as the main tool to gather the data. The use of a survey instrument creates various risks. First, surveys depend on the participant’s honesty and desire to share accurate personal information. Second, the questionnaires were distributed through the Internet using Google Forms. This means participants answered the survey by themselves without any assistance or opportunity to ask questions or clarification of key terms. This research method required clear and precise questions that had to be clearly understood by a pool of participants with diverse demographic backgrounds. Since the survey was sent electronically, there is no assurance everyone will fill out their survey. However, at the same time, using an online survey reduced the possibility of errors when exporting the results to the analysis software.

McCormac et al. (2017) warned that depending on self-reporting may result in data collection problems. The authors argued that due to the subjective nature of self-reporting, the data could have measurement errors. To mitigate data collection problems, they recommended not asking participants their name or their employer’s name. They argued that participants give more truthful answers if they are ensured anonymity and confidentiality.

Assumptions

The study relies on a survey instrument to gather the data. It is assumed that the participants followed an honor code and provided answers that were as truthful and demonstrated the closest representation of their beliefs and experiences as possible within the realm of the provided survey answer alternatives. It is also assumed that the participants had some knowledge or experience with information systems and had some basic understanding of the computer and security related terms used in the survey items.

Limitations

As the study was only to be shared with college student listservers from schools within the United States, this affects the generalization of the study regarding students from other countries and outside the traditional college student age group. Also, distributing the study via an online survey method may have affected the survey results. Students who have more technical knowledge are more likely to be part of the listservers that were used for the distribution and are more likely to answer an online survey.

Delimitations

Due to a large number of constructs and research questions in the model, the survey turned out long and was a reason to contemplate giving participants a reward for completing it. The survey questions were written in a clear and precise manner. The use of a panel of experts and a pilot study helped to validate a survey that had a reasonable length, with questions that were clear and precise, and provided the needed result data. Shneiderman et al. (2017) argue that survey instruments should be pilot tested before gathering the main research data. According to the authors, a pilot test is the best way to make sure a survey instrument is providing unbiased and reliable results.

Definition of Terms

Subjective Norm: According to Ng and Rahim (2005), it is what a person perceives as the social pressures that influence him to perform a given action.

Attitude Towards Knowledge Sharing: Bock et al. (2005) define it as how inclined a person is to share their knowledge with others.

Experience of Threat: Venkatesh et al. (2008) define it as an increased familiarity with a negative behavior or action.

Perceived Susceptibility: Liang and Xue (2009) define it as how probable a user was to be affected in a negative manner by an IS threat.

Perceived Severity: Liang and Xue (2009) define it as the perception of the user concerning the severity of the results of the IS threat.

Self-Efficacy: Ng and Rahim (2005) define it as the confidence a user has in his or her own ability to execute the threat mitigation processes.

Response Efficacy: Witte (1992) define it as how much an individual believes that a threat mitigation action will be effective against a specific threat.

Avoidance Motivation: Liang and Xue (2010) define it as how motivated a user will be to avoid an IT threat by performing or using the safeguarding measure or methods.

Threat Avoidance Behavior: Liang and Xue (2010) define it as a behavior or process that keeps the user in a specific security state the farthest away from an end state with an increased threat level.

List of Acronyms

AVE: Averaged Variance Extracted

FBI: Federal Bureau of Investigation

IT: Information Technology

IS: Information Systems

PLS: Partial Least Squares

TPB: Theory of Planned Behavior

TTAT: Technology Threat Avoidance Theory

Summary

The focus of the chapter is presenting and arguing for the validity of the research problem. It is argued that the examination factors influencing college students' security behavior involving interaction with peers should be studied. The problem necessitated the goal of empirically examining a research model of threat avoidance behavior in the context of ransomware security incidents among college students. This was studied by extending the TTAT with the factors subjective norm, attitude toward knowledge sharing, and experience of threat. A series of research questions and hypotheses were developed to test the extended model and its validity in answering the problem. Also, arguments were presented supporting the significance of why the study should be done. Finally, the barriers, limitations, assumptions, and delimitations were explained.

Chapter 2

Review of the Literature

Theory

The model is derived from the work done mainly by Liang and Xue (2010) which is built on Liang and Xue (2009). The research by Liang and Xue (2009) had the goal of building a model to understand the Information System (IS) threat avoidance behaviors exhibited by users of personal computers. From this study a model based on the TTAT was developed and empirically validated. The authors observed that avoidance motivation provides a satisfactory way to predict users' IS threat avoidance behavior. They concluded that avoidance motivation was affected by the constructs perceived threat, safeguard effectiveness, safeguard cost, and self-efficacy. Liang and Xue (2010) found that users only have threat perception if they think there is a real IS threat and that the threat has credible and negative consequences on their system.

The TTAT has the benefit that it is a general framework that has been found to be an effective way to explain the security related behaviors of IS users, even outside the enterprise setting. The TTAT models how users perceive the existence of a threat and what is the proper response to avoid it according to the available mitigation tools and actions. The model showed that users could be motivated by a perceived threat if the users are given insight on the magnitude of the damage the threat can cause and the probability of it happening (Liang & Xue, 2009).

In addition, two constructs are taken from the TPB: attitude toward knowledge sharing and subjective norm. Attitude toward knowledge sharing is derived from the attitude in the TPB (Ajzen, 1991). In comparison, the subjective norm is derived from the work of Ng and Rahim (2005). Ajzen (1991) stated that attitude was a strong predictor of a person’s intentions. According to their study, the personal aspect that attitude brings helps it become an even stronger factor than the subjective norm over a person’s behavior. Ajzen (1991) argues that unlike other frameworks, the role of the TPB is to explain why humans behave in a certain way.

Constructs

Subjective norm is a construct derived from the TPB. It is what people perceive as the social pressures that influence them to perform or not to perform a given action (Ng & Rahim, 2005). Subjective norms affect attitude toward knowledge sharing in a positive manner (Bock et al., 2005; Tu et al., 2015). There is a greater chance of exchange of information among individuals and thus a positive effect on the attitude toward information sharing if there is a subjective norm among an immediate social group.

Chan et al. (2005) argue that on average, individuals observe behavioral signals of others around them and imitate or follow that behavior. This herd behavior is amplified when the observing individual has little experience (Chua, 1980). Taylor and Todd (1995) called subjective norm a determinant behavior and argued that although it has an indirect effect on behavior, the effect was significant, and it is likely that subjective norms come before behavioral intentions.

Liang and Xue (2009) observed that subjective norm pressure and influence people but at the same time, it provides vital information that in prehistoric times could have meant the difference between life or death for the human. When humans observe others, they learn what behaviors, on average, would likely help them survive. Liang and Xue (2009) stated that these social pressures affect threat avoidance behavior and may help IS users predict the possible risks of any one of their actions and help them discern which mitigating action might produce the best result. In agreement with this finding, Tu et al. (2015) argued that an individual's coping intentions would be directly affected by social pressures. The authors also argue that when an individual's threat perception increases, the subjective norms act as a force that guides them to find a way to mitigate the perceived threat. However, the subjective norm can have a negative effect on human behavior. Chi et al. (2012) argued that subjective norms have a larger effect on a user's decision-making process than even perceived risk. Under enough pressure from their social group, some users yield and accept the use of systems or methods that they themselves perceived as risky.

In the TPB, attitude is defined as the general evaluation a person has of a given behavior (Ajzen, 1991). This is remarkably like attitude towards knowledge sharing. Attitude towards knowledge sharing has a positive association with perceived severity and perceived susceptibility. According to Bock et al. (2005), as more information is shared about a threat, there would be a probable increase in a user's perception of that threat's certainty of happening.

Tu et al. (2015) argued that going through negative experiences can increase the probability that a person becomes hypervigilant to that spectrum of threats in the future.

Users that have undergone a negative experience in the information systems domain would be more aware of the vulnerability in the future. When experience is gained, uncertainty is reduced, and the person would have a better sense of control over that behavior or action. Also, a person’s behaviors and actions become more intentional as experience is gained (Venkatesh et al., 2008). Experience of threat has a positive association with perceived susceptibility and perceived severity.

Liang and Xue (2009) described both perceived susceptibility and perceived severity in their model. They defined perceived susceptibility as how probable a user was to be affected in a negative manner by an IS threat. Perceived severity was defined as the perception of the user concerning the severity of the results of the IS threat. Also, users will begin searching for strategies to mitigate or cope with a potential threat as soon as the user perceives the threat (Liang & Xue, 2009). Liang and Xue (2010) demonstrate that the meta-constructs coping appraisal and perceived threat both have a positive effect on avoidance motivation.

According to Ng and Rahim (2005), self-efficacy can be defined as the confidence a user has in his or her own ability to execute the threat mitigation processes. While Johnston and Warkentin (2010) define it as how much the user thinks he or she has the required skill to execute recommended actions. Liang and Xue (2009) observed that if a user had a higher level of self-efficacy in the required method of guarding against IS threats, then the user would be more motivated to use the recommended method and protect himself against the potential threat. Liang and Xue (2010) show that self-efficacy has a positive effect on avoidance motivation.

Witte (1992) defines response efficacy as how effective an individual believes that a threat mitigation action is against a specific threat. The higher a person’s response efficacy, the more probable it is that the person will use a recommended action to defend against the perceived threat (Johnston & Warkentin, 2010). This means that response efficacy has a positive effect on avoidance motivation.

Liang and Xue (2010) define avoidance motivation as to how motivated a user avoids an IT threat by performing or using the safeguarding measure or methods. While Chen and Zahedi (2016), on the other hand, define avoidance as when users take actions such as reducing their Internet use to avoid security threats.

Building on the cybernetic theory of Edwards (1992), threat avoidance behavior is defined by Liang and Xue (2010) as behavior or process that keeps the user in a specific security state the farthest away from an end state with an increased threat level. Their study shows that avoidance behavior has a significant positive effect on threat avoidance behavior. Threat avoidance behavior is also part of a group of behaviors also known as adaptive coping. The behavior is described as one where the subject mitigates the threat in an effective manner (Chenoweth, Gattiker, & Corral, 2019).

Ransomware Threat

Since the first ransomware attack in 1989, the threat has become more dangerous and complex. During that first attack, the program would encrypt your files after the 90th computer reboot. It then went on to ask the user for a ransom of $189 and provided an address in Panama to send the money. In the last three decades since that first attack, ransomware is more complex, easier to hide, and faster to distribute through a victim’s computer networks (Nadir & Bakhshi, 2018).

Modern ransomware is not simply a single independent program that a victim downloads and that infects their computer, home, or office network and computers. Ransomware now depends on a complete infrastructure of VPNs, proxies, servers, and webhosts that are willing to look away while their networks are used for criminal acts (Richardson & North, 2017). According to Nadir and Bakhshi (2018), 57% of ransomware victims are now home users. These users are threatened and blackmailed not just with losing their encrypted data but also with the release of embarrassing photos or documents that will be made public or sent to their close friends and families. This change in targeting more individual users than enterprises, has to do with hacking groups noticing that individual users are more likely to pay the ransom and not inform the authorities. Individuals affected by ransomware pay an average of $300 for the key to decrypt their data (Richardson & North, 2017). The authors also note that ransomware hackers began using a dynamic pricing scheme that calculates ransoms according to the victim’s country. This technique helps the hackers maximize the ransoms paid and has allowed them to target poorer countries in the third world by asking for ransoms that are within the economic reality of the target’s location.

Han, Hoe, Wing, and Brohi (2017) mention that the WannaCry ransomware infected more than 200,000 computers in 150 countries. The authors note that in general, people do not report infections. The scare tactics and threats of releasing personal information keep many individual users from going to the authorities and reporting that they were hacked, and their computer was encrypted. The authors also observed that most of the users were infected while accessing sites that promised free movie streaming, trying to download through p2p services such as BitTorrent, or through phishing links.

The spread of modern ransomware is quick. Most of the newest and most aggressive ransomware encrypts not just the initial computer where the file was downloaded but also any other computer connected to the local network (Han et al., 2017). The authors recommend that individual users should be made aware of the dangers posed by ransomware and that best practices to protect themselves should be spread to social media.

University Information System Vulnerability

The WannaCry ransomware affected 150 universities around the world (Mohurle & Patil, 2017). University networks are especially vulnerable to computer security threats like ransomware. The network topography, campus size, and diverse userbase make university networks difficult to protect (Singh, Joshi, & Gaud, 2016). According to Patyal, Sampalli, Ye, and Rahman (2017), the University of Calgary was hit with ransomware once. Administration and faculty could not use their computers and students were ordered not to connect to the school's wireless Internet. The school paid the attackers a ransom of $15,000. Even after having paid the ransom and receiving the decryption keys, it took the University IT specialists ten days to repair the damage done and bring up the school's computer network and systems again.

Singh et al. (2016) warn that university computer networks have diverse attack vectors that are hard to defend due to several factors. First, university networks are mostly open networks with a large userbase. College campuses can be large and network security is even more complex when several geographically distant campuses are joined under a wide area network configuration. Also, some large university departments want to have their own locally managed decentralized internal network. This adds complexity to a network that needs to provide access to students, administrative staff, and professors; each with their own needs and permissions. In this environment, a ransomware infection from a student’s personal computer infects a large part of the university’s network within minutes.

Joshi and Singh (2017) argued that a university’s computer system environment has different attack vectors than the networks of other large enterprises such as banks. They also argue that the current security guidelines used by universities are not effective in defending against modern threats such as ransomware.

College Student Information System Threat Behavior

Howarth (2014) argued that 95% of all computer security incidents are caused by errors rooted in the human factor. Diaz, Sherman, and Joshi (2020) studied how college students would respond to phishing attempts. In the phishing test, the authors found that 92% of the students opened the email and 59% of those who opened the email went on to click the link. The authors then compared how the clicking rate varied across the different schools and departments of the university. The Non-STEM students had higher click rates than the STEM students. And within the STEM students, the Engineering and Computer related majors had the lowest click rates.

Diaz et al. (2020) also observed older students clicked less on the phishing email than the younger students. The authors did not find any difference in phishing avoidance among the genders. Finally, they concluded that student’s general lack of awareness of phishing emails might be problematic for universities’ IT security. Also, the authors believe the students may have been overstating their knowledge as there was a discrepancy in the phishing click rates and the security knowledge the students said they had.

Chapter 3

Methodology

Overview

A quantitative method is used for this study. The data was gathered using a survey instrument which was developed by combining items from surveys that have been empirically validated by previous studies. This new survey was used to gather the data required to study the effects of the factors that influence the threat avoidance behavior in ransomware security incidents among college students. The survey method allows for a fast and efficient means of gathering information. Using electronic surveys provides benefits similar to those of postal surveys, including the reduction of bias. Since, there would not be an opportunity to explain the instructions or clarify definitions to the volunteer in person, the questions must be straightforward (Holt, 1997).

Development of Survey Instrument

The survey used the 7-point Likert scale, as it could be more precise than other scales (A. Joshi, Kale, Chandel, & Pal, 2015). They mention that 7-point scales give participants more options and this means that people would be most likely to find the answer closest to their individual perception of the situation in the questionnaire. The only exception is the experience of threat construct, which is a binary item as per Tu et al. (2015).

Table 1 outlines the 48 survey items developed to measure the degrees of the constructs in the study. The construct name and an abbreviation for each item are given. Also, the descriptions are the actual item statements that were answered by the participants. Lastly, Table 1 includes the citation of the source from where the survey item is taken and the construct's composite reliability, which measures the internal consistency.

Table 1

Survey Items Descriptions and Sources

Construct Name	**Description**	**Survey Item Reference**	**Composite Reliability**
Subjective Norm		(Bock et al., 2005)	0.8230
SN1	My university IT Dept thinks that I should share my anti-ransomware knowledge with other students.		
SN2	My professors think that I should share my anti-ransomware knowledge with other students.		
SN3	My friends think I should share my anti-ransomware knowledge with other students.		
SN4	Generally speaking, I try to follow the University's IT security policy and intention.		
SN5	Generally speaking, I accept and carry out my friends security ideas and suggestions even though they are different from mine.		
SN6	Generally speaking, I respect and put into practice my friends' security practices.		
Attitude Toward Knowledge Sharing		(Bock et al., 2005)	0.9184
ATTK S1	My anti-ransomware knowledge sharing with other students is good.		
ATTK S2	My anti-ransomware knowledge sharing with other students is an enjoyable experience.		

ATTKS3	My anti-ransomware knowledge sharing with other students is valuable to me.		
ATTKS4	My anti-ransomware knowledge sharing with other students is a wise move.		
Experience of Threat		(Tu et al., 2015)	‘Binary’
EOT1	Have you had a ransomware infection in the past?		
Self-Efficacy			
	I could successfully install and use anti-ransomware software if …	(Liang & Xue, 2010)	0.957
SE1	… there was no one around to tell me what to do		
SE2	I had never used a software like it before		
SE3	I had only the software manuals for reference		
SE4	I had seen someone else doing it before trying it myself		
SE5	I could call someone for help if I got stuck		
SE6	.. someone else helped me get started		
SE7	I had a lot of time to complete the job		
SE8	I had just the built-in help guide for assistance		
SE9	.. someone showed me how to do it first		
SE10	I had used similar software like this one before to do the job		
Response Efficacy		(Johnston & Warkentin, 2010)	0.897
RE1	Anti-ransomware software works for protection		
RE2	Anti-ransomware software is effective for protection		
RE3	When using anti-ransomware software, a computer is more likely to be protected		
Perceived Severity		(Liang & Xue, 2010)	0.945

PS1	Ransomware would delete my personal information from my computer without my knowledge		
PS2	Ransomware would invade my privacy		
PS3	My personal information collected by ransomware could be misused by cyber criminals		
PS4	Ransomware could record my Internet activities and send them to unknown parties		
PS5	My personal information collected by ransomware could be subject to unauthorized secondary use		
PS6	Ransomware would slow down my Internet connection		
PS7	Ransomware would make my computer run more slowly		
PS8	Ransomware would cause a system crash on my computer from time to time		
PS9	Ransomware would affect some of my computer programs and make them difficult to use		
Perceived Susceptibility		(Liang & Xue, 2010)	0.972
PSU1	It is extremely likely that my computer will be infected by ransomware in the future.		
PSU2	My chances of getting ransomware are great.		
PSU3	There is a good possibility that my computer will have ransomware.		
PSU4	I feel ransomware will infect my computer in the future.		
PSU5	It is extremely likely that ransomware will infect my computer.		
Avoidance Motivation		(Liang & Xue, 2010) (Chen & Zahedi, 2016)	0.977 0.94
AM1	I intend to use anti-ransomware software to avoid ransomware		
AM2	I predict I would use anti-ransomware software to avoid ransomware		

AM3	I plan to use anti-ransomware software to avoid ransomware		
AM4	I intend to periodically use anti-ransomware software to protect my computer from ransomware.		
AM5	In the immediate future I intend to customize my browser and computer settings to prevent the intrusion of ransomware on my computer.		
AM6	In the near future, I intend to check my computer for the presence of ransomware.		
Threat Avoidance Behavior		(Liang & Xue, 2010) (Yoon, Hwang, & Kim, 2012)	0.920 0.75
TAB1	I run anti-ransomware software regularly to remove ransomware from my computer.		
TAB2	I update my anti-ransomware software regularly.		
TAB3	I immediately delete suspicious emails without reading them.		
TAB4	Under no circumstance would I ever open a USB drive without running a ransomware scan.		

Survey Instrument Validation

Once the preliminary survey was developed, the next step was to bring together 4-6 subject matter experts to be part of the expert review panel. The panel's main task was to validate each survey item's relevance to the definitions of the constructs (Sireci & Faulkner-Bond, 2014). Based on the feedback from the panel, the final wording and structure were modified. After recommendations by the panel, the next step was to pilot test the survey with 20-25 college students. The goal of the pilot study was to evaluate the survey for clarity, ease, and to have an estimate of how much time it took to complete. The results of this pilot test were also empirically analyzed to validate the survey and make sure the correct data was gathered. According to Shneiderman et al.

(2017), survey instruments should be pilot tested before gathering the main research data. The authors argued that a pilot test is the best way to confirm a survey instrument is providing unbiased and reliable results.

Data Collection

The target group from which data was collected are individual students from United States universities. The study used a non-probability sampling design, specifically judgment sampling which is an extension of the convenience sampling method. This method is preferred since data is being gathered from college students (Sekaran & Bougie, 2016). Students were invited to participate voluntarily in the study by sending invitations with the survey link to public email listservers. One example of these listservers is the Hispanic in Computing group through which invitations to participate in studies, scholarships, and workshops are constantly shared with hundreds of students from universities across the nation. Sending messages through these groups does not require special permissions from the owners and at no moment is personally identifiable information required as messages are sent to a specific general account that then forwards the messages to the group members. The available listservers had a reach of more than 1,500 students from United States universities.

In the study by Trespalacios and Perkins (2016), students responded to the online invitation on average of 23% to 26%. The authors found no significant difference in participation rates between invitations that were personalized or not. Also, Johnston and Warkentin (2010) were able to achieve a 40% response rate without giving any incentives. In their study, 73% of the respondents were in the 18-29 demographic. The computer focused email listservers that were targeted are made up of highly engaged students that continuously participate in group topics.

Ringle, Sarstedt, and Straub (2012) argue that to have reliable results when using PLS-SEM, it is important to have an acceptable level of measurement. Although many researchers using PLS-SEM use the rule of ten or five to determine the sample size, this calculation should only be used as a rough guideline and should be verified with more precise power analysis software or by using Cohen (1992) power tables (Hair, Ringle, & Sarstedt, 2011). Although PLS-SEM has demonstrated usefulness with small sample sizes, Kante, Chepken, and Oboko (2018) argue that depending on complexity, studies using PLS-SEM should have a sample size of at least 200 participants.

To have an estimate of the sample size, the rule of ten could be used. According to Hair Jr, Hult, Ringle, and Sarstedt (2016), the largest number of formative indicators measuring a construct would be multiplied by 10. Construct Self-Efficacy has ten indicators, resulting in 100 when multiplied by 10. However, to have a precise estimate of sample size, the G*Power Version 3 software was used (Faul, Erdfelder, Lang, & Buchner, 2007). Using an effect size of 0.25, an error probability of 0.05, and a power of 0.95, G*Power calculates a sample size of 164 participants. This number is also near the number of participants studied in Liang and Xue (2010), 152. Based on all the considerations, the safer sample size for this study was 164.

Data Analysis Plan

The goal was to analyze the data gathered from surveys completed by college students for measurement validation and hypothesis testing. The data analysis follows the tests and methods used by Liang and Xue (2010) with PLS-SEM.

Once the data collection phase was complete, the data underwent a pre-analysis data screening. During this phase, the collected data were checked for missing data, suspicious patterns, outliers, and data distribution. Concerning data distribution, Hair Jr et al. (2016) point out that although PLS-SEM does not require normally distributed data, it should still be checked in case the data is extremely non-normally distributed. Once the data is ready for analysis, SmartPLS3 was used for the main analysis. According to the recommendation of Fornell and Bookstein (1982), Partial Least Squares (PLS) is chosen as an analysis method because it was found to be more robust when testing complex structural models. This method is also useful for the prediction of the impact independent variables have on the dependent variable. PLS also has the benefit that a valid analysis can be done with smaller sample sizes. In the study by Ringle et al. (2012), 36% of the researchers surveyed said they preferred to use PLS because it allowed them to run tests in small sample sizes.

Testing Measurement Model

The goal of the measurement model is to test the relationship between the latent variables and the observed data. The validation of the measurement model was performed by following the steps taken by Liang and Xue (2010) to determine the convergent and discriminant validity of the constructs. According to Hair Jr et al. (2016), convergent validity tests whether constructs that are expected to be related really are related. Discriminant validity tests whether constructs that are expected to be unrelated really are unrelated. The testing criteria for the convergent construct validity Liang and Xue (2010) used was that items should have a higher weight load per item on the hypothesized construct when compared to other constructs. While for the discriminant validity test; building on the recommendation by Fornell and Bookstein (1982); the criteria used was that the square root of the construct's averaged variance extracted (AVE) has to be larger than the correlations with the other constructs being tested. A PLS confirmatory analysis was done to calculate the item loadings and the constructs AVE were calculated. Also, Cronbach's alpha was calculated to measure the internal consistency of the items and if the result is over 0.70 then the model has the necessary measurement reliability (Hair Jr et al., 2016). Finally, model fitness was determined using the SmartPLS standardized root mean square residual method. The method output reveals differences between observed and expected model correlations. The model would be considered a good fit if the values are between 0.08 and 0.10.

Testing Structural Model

The study verified how subjective norm, attitude toward knowledge sharing, the experience of threat, perceived severity, perceived susceptibility, self-efficacy, and response efficacy affect each other. The study used the following as control variables; age, gender, and internet experience. The goal of the structural model test was to analyze the relationship between the latent variables. These relationships connect the input and output of the model. The arrows connecting the constructs represent the structural hypothesis of the model.

To determine how constructs affected one another, this study calculated the beta coefficients. The beta coefficients of the PLS structural model are also known as the standardized regression coefficients. These values are calculated by performing SEM-PLS analysis on standardized values. This process allowed the analysis of the effect of independent variables on the dependent variable even if the data has values in different measurement units (Sekaran & Bougie, 2016). The R^2, path coefficients, and significance of the coefficients of the structural relationships were calculated. In PLS-SEM for the path coefficient to be significant in a two tailed t-test, the t-value > 1.95. This value gave us a $p<0.05$. These *p*-values of a structural path can be calculated in SmartPLS through the process of bootstrapping (Hair Jr et al., 2016). Bootstrapping is a resampling technique that tests the coefficients’ significance.

Resources

A survey instrument was used to gather the required data. The survey was created using the Google Forms application that is part of the Google Docs suite of Office Applications. The Google Docs suite of Office Applications is a free web-based application. Once the data was gathered, SmartPLS3 and SPSS were used to analyze the data. All the required resources were obtainable when required.

Chapter 4

Results

Pilot Study Expert Panel

During September and October of 2020, a group of four volunteers with academic and professional experience in information system security accepted the invitation to be my Expert Panel and evaluate the survey instrument.

The volunteers were provided with a copy of the dissertation abstract, the survey, and a rubric with which to evaluate the survey. The title of the rubric is “Survey/Interview Validation Rubric for Expert Panel” (VREP). It was created by Marilyn K. Simmon and Jaquelyn White (White & Simon, 2011). The goal of the rubric is to include criteria that measure face validity, construct validity, and content validity. The rubric uses a 4-point scale ranging from a 1 (Not Acceptable – major modifications needed) to a 4 (Exceeds Expectations – no modifications needed). The criteria measured are as follows: clarity, wordiness, negative wording, overlapping responses, balance, use of jargon, appropriateness of responses listed, use of technical language, application to praxis, relationship to the problem, and survey adequately measures each construct. These metrics were answered for each individual construct evaluated. The rubric has a total of 19 criteria.

The experts evaluated the survey measurement items, and we then discussed their thoughts and recommendations about the survey items. Most of the experts scored the majority of the criteria with a 4. A score of 3 was mainly given to negative wording, overlapping responses, clarity, and wordiness. None of the criteria scored in the twos or ones or required their recommendations with respect to the validity of the actual questions and constructs. The main recommendations focused on making changes to the format of the survey, dividing it into pages instead of one long page, and changing words in several questions to improve the clarity/readability. One of the experts asked about the similarities of two sets of questions and the possibility of removing one of each. However, after discussing the goal of the questions and the testing of answer validity, the expert did not recommend the removal. To improve clarity and readability, I divided the survey into more sections to limit the number of items per page. Also, periods were added at the end of each item statement. The experts also recommended the addition of two demographic questions: 1) Are you enrolled in a computing related major? 2) Are you aware of your University's IT security policies?

The four experts are bilingual and have complete fluency in the English language. However, they are non-native English speakers. This allowed them to give me additional feedback regarding the clarity of the items that a native speaker would not have provided. For example, one of the panelists mentioned that the double negative in items AM4 to AM6 was difficult to understand and forced her to reread them several times in order to understand them. Therefore, it was decided to eliminate these three items and to also delete ATKS2. In addition, items TAB3 – TAB6 were moved to Avoidance Motivation. As three items from Threat Avoidance Behavior were moved to Avoidance Motivate, only two items were left to measure Threat Avoidance Behavior. This required adding two new items to Threat Avoidance Behavior to have four items measuring the construct.

The data from the rubric was added to SPSS and reliability statistics analyses were run. SPSS ran the reliability statistics on 10 of 19 metrics as the other 9 had zero variance. The test calculated a Cronbach's Alpha based on the standardized items of 0.708 which means there is an acceptable internal consistency.

Pilot Study Analysis Results

Between the months of November and December 2020 a pilot study was completed to determine flaws in the planned methods and to observe possible response rates. At the end of the established pilot study, there were a total of 16 participants in the survey. Every single one of the participants filled out all questions. There was no missing data in the result file.

The number of participants was lower than expected. The invitations were sent to various email listservs that are known to have high participation rates. It is suspected that in situations relating to the Covid-19 pandemic and the highly unusual university semesters that were and are currently in session, students might not have been as motivated as usual to complete a survey at the end of their semester. The mitigation plan was to send the survey to additional listservs along with reminders.

The pilot study data was added to SPSS. The results of the Descriptive Statistics, the Cronbach's Alpha, and the bar charts with the demographics are shown in Appendix D. To test for construct reliability, the Cronbach Alpha of each set of items making up the constructs was also calculated. Avoidance motivation resulted in a coefficient of 0.968, Attitude Towards Knowledge Sharing had a coefficient of 0.819, Perceived Severity had a coefficient of 0.937, Perceived Susceptibility of 0.932, Response Efficacy of 0.906, Self- Efficacy of 0.746, Subjective Norm of 0.789, and Threat Avoidance Behavior of 0.725. Since Experience of Threat has only one item, its coefficient is 1.00. Because all the Cronbach Alpha values are greater than 0.7, all of the constructs have internal consistencies that are acceptable.

Main Study Analysis Results

The data for the main study analysis was gathered during the month of March 2021. According to the calculation done using G*Power, the recommended minimum number of participants was 164. Data were gathered from a total of 174 participants. As seen during the pilot test data gathering period, getting the required number of participants was no easy task. The combination of hybrid or purely online learning due to the pandemic and the different Spring Break Holiday periods throughout United States universities during the month of March was a large obstacle to the data-gathering effort. As anecdotal reports have observed, students did not seem as motivated as they have been in the past to participate in online surveys, although this topic is for a different study that is outside of the scope and the domain of the present dissertation. To mitigate the low participation rate seen in the pilot study, the invitations were sent to more email distribution listservs and an increased number of reminders were sent to invite students to participate in the study.

The data from the main study was added to SPSS for cleanup and pre-analysis tasks. The results of the Descriptive Statistics, the Cronbach's Alpha, normality, Mahalabonis distance and outlier test, and additional charts were added to Appendix E. Table 2 has a summary of the demographic data.

Table 2

Demographic Data (N=174)

Data Items	Frequency	Valid Percent	Cumulative Percent
Age			
18-25	97	55.7	55.7
26-35	50	28.7	84.5
36-45	13	7.5	92.0
46-55	12	6.9	98.9
56-65	1	0.6	99.4
Over 65	1	0.6	100
Sex (N = 173)			
Male	53	30.6	30.6
Female	115	66.5	97.1
Prefer not to say	6	2.9	100
How many years have you been using the internet?			
5 years or less	4	2.3	2.3
6-10 years	37	21.3	23.6
11-15 years	59	33.9	57.5
Over 15 years	74	42.5	100
Are you enrolled in a computing-related major?			
Yes	52	29.9	29.9
No	122	70.1	100
Are you aware of your University’s IT Security Policies?			
Yes	84	48.3	48.3
No	90	51.7	100

The age distribution of the survey participants was the following: 97 students out of 174 were between 18 and 25 years old, 50 were between 26 and 35 years old, 13 were between 36 and 45 years old, 12 were between 46 and 55, one student was between 56-65, and one was over 65. The sex distribution of the participants was as follows: 53 students were male, 115 were female, five preferred not to say, and one participant did not provide an answer and left it blank. It should be clarified that this was the only instance of a blank value in the data set.

Concerning the question about their years of internet experience, participants answered the following: 74 participants said they had over 15 years of internet experience, 59 said they had 11-15 years of experience, 37 said they had 6-10 years of experience, and four said they had five years or less of internet experience. On the question asking if the students were aware of their university’s IT security policies, 90 answered no and 84 answered yes. Finally, on the question that asked if they were enrolled in a computing related major, 122 students said no and 52 said yes.

As expected, most of the volunteers were traditional college age students in the 18-25 years old range. However, surprisingly, a substantially larger number of female students answered the survey than male students. This could be in part due to the composition of the listservs where the survey participation invitations were sent to. Also, a majority of students said that they were aware of their universities’ IT security policies. At the same time, most of the participants were not from a computer related major. This last detail is important because it means that the survey was answered by a more technically diverse population than having only computer savvy computer majors answer the survey and provides more generalizable answers.

To test for outlier cases, the Mahalanobis distance was calculated using the linear regression analysis in SPSS. No case with outlier data was found in the dataset.

To test for item internal consistency, Cronbach’s Alpha is calculated using SPSS. All variables except for Experience of Threat were tested as this variable is Boolean. All variables except for Threat Avoidance Behavior were above the threshold of 0.700 to satisfy the reliability test. However, Cronbach’s Alpha for Threat Avoidance Behavior was 0.692 which is close to the 0.700 thresholds. The data for Cronbach’s Alpha can be observed in Table 3.

Table 3

Cronbach’s Alpha

Variable	**Number of Items**	**Cronbach’s Alpha**
Attitude Towards Knowledge Sharing	4	0.876
Subjective Norm	6	0.784
Response Efficacy	3	0.895
Self-Efficacy	10	0.842
Perceived Severity	9	0.923
Perceived Susceptibility	5	0.884
Avoidance Motivation	6	0.928
Threat Avoidance Behavior	4	0.692

The main data analysis was done using SmartPLS. The goal of the first part of the analysis with SmartPLS is to test the measurement model. More information on bootstrapping can be found in Chapter 3’s section on Testing Structural Models. In these analyses, bootstrapping was performed to assess the path coefficients’ significance by resampling the collected data. SmartPLS is configured to do 2,000 subsamples during the bootstrapping procedure and then subsequently performed factor analysis. Once the calculation is complete, outer loadings verify the estimates calculated for the relationships of the survey measurement items to corresponding constructs in the model. The result tells us how much an item contributes to the construct to which it has been assigned. This process is iterative and is run several times until only items that have outer loading values over 0.7 remain. Each model construct was further dissected into survey statement items and each of these items was tested independently within the model construct. All survey statement items were identified to be significantly different from null expectations. The loadings reported in Table 4 are the regression coefficients to the scores upon which the t-statistics are calculated. Loading values of about 0.7 are considered to explain more than 50% of the indicator's variance. Any items that were identified as having a loading value below 0.7 were excluded from further analyses. The calculated *p*-values were used to accept or reject the null hypotheses with respect to the measurement model test. It was observed that the t-statistic values were consistent across model constructs except for four self-efficacy items and two of the perceived severity Items. However, the variance in these two constructs did not change the associated *p*-values.

Table 4

Measurement Model Testing Results

Construct	**Item**	**Loading**	**t-statistics**	***p*-values**
Subjective Norm	SN1	0.877	27.941	< 0.001
	SN2	0.922	42.955	< 0.001
	SN3	0.887	54.820	< 0.001
Attitude Towards Knowledge Sharing	ATTKS1	0.827	23.982	< 0.001
	ATTKS2	0.867	29.630	< 0.001
	ATTKS3	0.894	40.830	< 0.001
	ATTKS4	0.828	21.705	< 0.001

Self-Efficacy	SE3	0.710	3.313	< 0.001
	SE4	0.820	4.478	< 0.001
	SE8	0.858	4.512	< 0.001
	SE10	0.720	3.345	< 0.001
Response Efficacy	RE1	0.917	46.347	< 0.001
	RE2	0.921	54.331	< 0.001
	RE3	0.888	31.146	< 0.001
Perceived Severity	PS4	0.727	6.858	< 0.001
	PS5	0.702	6.553	< 0.001
	PS6	0.886	20.783	< 0.001
	PS7	0.900	17.763	< 0.001
	PS8	0.919	18.529	< 0.001
	PS9	0.870	15.421	< 0.001
Perceived Susceptibility	PSU1	0.715	12.207	< 0.001
	PSU2	0.834	20.773	< 0.001
	PSU3	0.849	28.751	< 0.001
	PSU4	0.871	26.063	< 0.001
	PSU5	0.867	30.698	< 0.001
Avoidance Motivation	AM1	0.893	46.163	< 0.001
	AM2	0.859	32.238	< 0.001
	AM3	0.902	43.404	< 0.001
	AM4	0.865	23.508	< 0.001
	AM5	0.833	30.854	< 0.001
	AM6	0.796	25.489	< 0.001
Threat Avoidance Behavior	TAB1	0.929	64.923	< 0.001
	TAB2	0.910	38.421	< 0.001
Experience of Threat	EOT1	1	0	1

Before the PLS test is run to test the structural model, the discriminant validity should be verified using the Fornell-Larcker Criterion. As shown by the results in Table 5 all are within the correct ranges and demonstrate that no two constructs are correlating and are measuring correctly different concepts correctly.

Table 5

Discriminant Validity

	ATTK	AM	EOT	PS	PSU	RE	SE	SN	TAB
TTK	0.854								
AM	0.262	0.859							
EOT	-0.186	-0.176	1						
PS	-0.012	0.015	-0.227	0.838					
PSU	0.2	0.318	-0.191	0.045	0.83				
RE	0.163	0.338	-0.019	0.08	0.064	0.909			
SE	0.018	0.156	-0.002	0.117	-0.201	0.216	0.779		
SN	0.518	0.102	-0.05	0.056	0.125	0.093	0.141	0.896	
TAB	0.148	0.648	-0.122	0.058	0.316	0.171	0.011	0.084	0.9191

Table 6 shows the composite reliability calculated through SmartPLS. All of the composite reliabilities are within the acceptable parameters of greater than 0.700.

Table 6

Composite Reliability

Relationship	**Composite Reliability**
Threat Avoidance Behavior	0.916
Subjective Norm	0.924
Self-Efficacy	0.860
Response Efficacy	0.934
Perceived Susceptibility	0.917

Perceived Severity	0.934
Experience of Threat	1
Avoidance Motivation	0.944
Attitude Towards Knowledge Sharing	0.915

Since the measurement model is satisfied for PLS-SEM analysis, the structural model was used to test the hypotheses. Figure 2 shows the PLS-SEM model with the appropriate R-squared values. The 42% variance of threat avoidance behavior is explained by the constructs in the research model. Table 7 shows the path coefficients for the model. In this table I can evaluate the *p*-values for the different relationships in the model. The model shows that the relationship between subjective norm and response efficacy is not significant. Equally significant relationships are found between perceived susceptibility and avoidance motivation and response-efficacy and avoidance motivation.

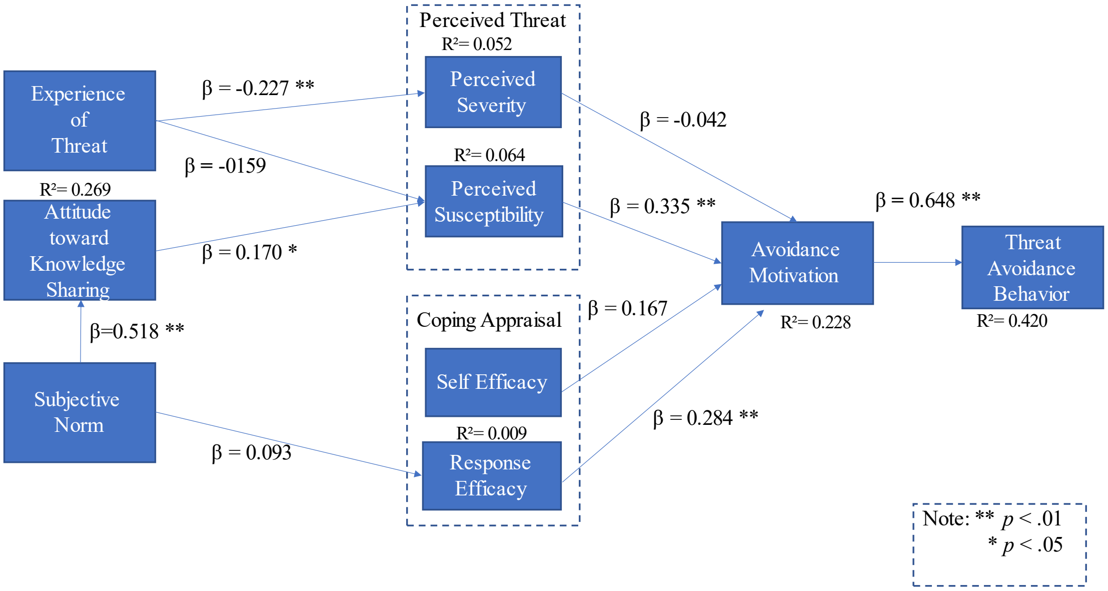


Figure 2. PLS-SEM Analysis Result

H1 is supported as subjective norm has a positive effect on attitude towards knowledge sharing (β = 0.518, *p* < .001). *H2* is not supported as experience of threat did not have a positive effect on perceived severity (β = -0.227, *p* < .001). The coefficient is negative, indicating the relationship is negative. *H3* is not supported as experience of Threat had a negative effect on perceived susceptibility, because the coefficient is negative (β = -0.159, *p* = 0.062). *H4* is supported as attitude towards knowledge sharing had a positive, although small, effect on perceived susceptibility (β = 0.0.17, *p* = .05). *H5* is not supported as the positive effect of subjective norm on response efficacy was found to be minimal and of no significance (β = 0.093, *p* = 0.211). *H6* is not supported as a negative effect measured between perceived severity and avoidance motivation was not of significance (β = -0.043, *p* = 0.542). *H7* is supported as there is a positive and significant effect of perceived susceptibility on avoidance motivation (β = 0.336, *p* < .001). *H8* is not supported as there is a positive effect by self-efficacy on avoidance motivation and the level of significance nears the significant threshold (β = 0.167, *p* = 0.059). *H9* is supported as response efficacy was found to have a positive effect on avoidance motivation (β = 0.284, *p* < .001). *H10* is supported as avoidance motivation was found to have a positive effect on threat avoidance behavior (β = 0.648, *p* < .001).

Table 7

Structural Model Testing Results

Hypothesis	**Path**	**Coefficient**	**t-statistics**	***p*-values**	**H Supported?**
H1	Subjective Norm → Attitude Towards Knowledge Sharing	0.518	8.967	< 0.001	Supported
H2	Experience Of Threat→ Perceived Severity	-0.227	3.813	< 0.001	Not Supported

H3	Experience Of Threat→ Perceived Susceptibility	-0.159	1.865	0.062	Not Supported
H4	Attitude Towards Knowledge Sharing→ Perceived Susceptibility	0.17	1.961	0.050	Supported
H5	Subjective Norm→ Response Efficacy	0.093	1.252	0.211	Not Supported
H6	Perceived Severity→ Avoidance Motivation	-0.043	0.061	0.542	Not Supported
H7	Perceived Susceptibility→ Avoidance Motivation	0.336	4.689	< 0.001	Supported
H8	Self-Efficacy→ Avoidance Motivation	0.167	1.893	0.059	Not Supported
H9	Response Efficacy → Avoidance Motivation	0.284	4.368	< 0.001	Supported
H10	Avoidance Motivation → Threat Avoidance Behavior	0.648	13.098	< 0.001	Supported

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

The goal of this dissertation research was to empirically examine threat avoidance behavior in the context of ransomware security incidents among college students. This was done by extending the Technology Threat Avoidance Theory with the addition of the factors subjective norm, attitude toward knowledge sharing, and experience of threat. These factors were chosen to determine whether social pressures and previous experiences of threat can influence avoidance behavior.

Data for this study was gathered from 174 participants in United States colleges during March of 2021. During the testing of the measurement model using SmartPLS, it was observed that various constructs had items with outer loadings that were under the 0.7 threshold (Hair Jr et al., 2016). These items were removed, and the analysis was run again. This procedure improved the model analysis.

The research also had seven research questions. Concerning the first question, subjective norm was observed to have a positive effect on attitude towards knowledge sharing. People with higher levels of subjective norm would be more likely to share their knowledge about ransomware infections with friends. In the second question, experience of threat had negative effects on both constructs that make up perceived threat; perceived severity and perceived susceptibility. Experience of threat was expected to have a positive effect on perceived threat, however it did not. This unexpected result deserves further study in the future. The third question concerns the effect of attitude towards knowledge sharing on perceived threat. The results revealed that a positive but small effect on perceived susceptibility. In the fourth question, subjective norm was observed to have no significant effect on response efficacy. The fifth question concerns the effect of perceived threat on avoidance motivation. Perceived threat is made up of perceived severity and perceived susceptibility. The research showed that only one of the constructs, perceived susceptibility, had a positive effect on avoidance motivation; while perceived severity had a minimal negative effect that is not significant. The sixth question is about the effect of coping appraisal on avoidance motivation. Coping appraisal is made up of the constructs self-efficacy and response efficacy. The research showed that only one of the constructs had a positive effect on avoidance motivation. However, the effect of response efficacy was significant, while the effect of self-efficacy was small and of no significance. The last question is about how avoidance motivation affects threat avoidance behavior. The research showed that avoidance motivation had a strongly significant effect on threat avoidance behavior.

Of the 10 hypotheses, five of them were not supported by the results: H2, H3, H5, H6, and H8. H2 stated that experience of threat would have a positive effect on perceived severity while H3 stated that experience of threat would have a positive effect on perceived susceptibility. However, the observed effect was the opposite. H2 and H3 were based on (Tu et al., 2015). This study argued that individuals that underwent through some kind of threat would then become hypervigilant about that threat in case it appeared again in the future. It is of particular interest, that in the study, experience of threat was positively associated with both constructs that make up perceived threat. However, in my research, the opposite relationship was observed; experience of threat had a negative effect on both constructs that make up perceived threat. This demonstrates that there might be a problem with the items used to measure the constructs that produced an unexpected result.

H5 stated that subjective norm would have a positive effect on response efficacy. Again, the effect observed in this relationship was the opposite. Tu et al. (2015) argued that social influences directly influence an individual’s coping intentions. Chi et al. (2012) observed that subjective norm would have a greater effect on individuals who perceived risk. However the contradiction with my findings could be related to what was observed by Chua (1980). That study found that subjective norm does influence individual behaviors, but the author found a very particular caveat. The effect would be observed mostly in individuals who had little experience and had yet to adopt a particular attitude or mindset. This is an important detail because 42% of the survey participants said that they had over 15 years of internet experience. This large amount of experience could have affected the relationship between subjective norm and response efficacy since people with more experience are less affected by subjective norm.

H6 stated that Perceived Severity would have a positive effect on avoidance motivation. However, the opposite was observed. Liang and Xue (2010) observed that perceived threat had a positive effect on avoidance motivation. perceived threat is composed of the constructs perceived severity and perceived susceptibility. In this study, only perceived severity had a negative effect while perceived susceptibility had a positive effect on avoidance motivation.

H8 stated that self-efficacy would have a positive effect on avoidance motivation. In this study, the effect of self-efficacy was small and not significant. Liang and Xue (2010) observed that coping appraisal had a positive effect on avoidance motivation. Coping appraisal is composed of the constructs self-efficacy and response efficacy. In this study, self-efficacy had a small effect on avoidance motivation that was not of significance, while response efficacy had a larger and significant positive effect.

Although avoidance motivation had the expected effect as seen in previous research that validated the model used, it is interesting to observe that perceived threat and coping appraisal did not produce results as expected. Previous research stated that both constructs would have a positive effect on avoidance motivation, but this was not the result. Only one of the two constructs that make up each one was found to have a significant and positive effect on avoidance motivation.

Also, the constructs that were added to the Liang and Xue (2010) had mixed results. subjective norm was not found to have a strong or significant effect on response efficacy. This could be caused by the fact that 42% of survey participants were experienced and the more experience a person is, the less they are affected by subjective norm (Chua, 1980). However, subjective norm did behave as expected with a strong positive effect on attitude toward knowledge sharing. This last construct had a significant but weak positive effect on perceived susceptibility. The biggest outlier was experience of threat. It was expected that this construct would have a strong and significant effect on perceived threat, but the opposite was observed.

Implications and Recommendations

Ransomware is becoming an increasing threat to information system users. At the same time, college students have been largely ignorant of their relative risk for becoming victims of ransomware infections. This study expanded the TTAT to better understand the perceptions and behaviors of college students towards ransomware threats by using three additional features: subjective norm, attitude toward knowledge sharing, and experience of threat. The TTAT explains how individual IT users engage in threat avoidance behaviors. The study validated the effect of avoidance motivation on threat avoidance behavior as seen in previous TTAT literature. Also, response efficacy and perceived susceptibility was found to have the expected effects on avoidance motivation. However, perceived severity and self-efficacy did not behave as expected. While Experience of threat had a significant and negative effect on perceived severity, self-efficacy was not affected by any of the extending features. The unexpected results in some of the constructs should be studied further to determine why the behavior was so different in comparison to the literature.

The study showed that attitude towards knowledge sharing increased perceived susceptibility, which then leads to avoidance motivation. This suggests that even in students with high levels of inherent knowledge about threat avoidance, perceived susceptibility was sufficient to have a positive effect in threat avoidance behavior. In addition, this study found that several of the proposed hypotheses were supported. Subjective norm was observed to have a positive effect on attitude towards knowledge sharing. One explanation for this is that the participants had a high understanding of threat avoidance behaviors, although this could have biased the expectations that they might be more significantly influenced by subjective norms.

This study provides clear information on how college students understand the risk of ransomware to their computer systems, how they obtain knowledge about risk, identify threats within their surroundings, and how they avoid those risks.

Limitations and Future Studies

The scope of this research was limited to the study of threat avoidance behavior of United States college students in the context of ransomware infections. Inviting only students from the United States affects the generalization. First, other countries have different threat levels of ransomware infection; be it because of less computer security knowledge or different availability of software tools to protect the systems. Also, different countries may have various levels of threat avoidance behavior as there are different levels of risk behaviors among societies.

Another limitation of the study was the data collection method. The data was collected as a web-based survey. Web based surveys have several biases such as self-selection, desirability, and acquiescence bias. And lastly, a limitation that cannot be ignored is the time frame during which the data was gathered. Starting in the year 2020, the world has been operating under the stress and preoccupation of the Covid-19 pandemic. The pandemic forced governments to order shutdowns including the closure of on-site college education in most of the world. This has changed how students work and learn. It can be surmised that the constant presence of Covid-19 on students’ minds may affect, first; the desire of students to spend time completing an online web survey. And second it may have affected the answers of those who volunteered and completed the survey. It is possible that some of the answers would have been different during a less stressful time for the survey volunteers.

Summary

The main objective of this research was to examine threat avoidance behavior in the context of ransomware security incidents among college students by way of extending an existing framework, the Technology Threat Avoidance Theory. The introduction of the study provided background and foundation for the domain and the research problem that the study focuses on. Hypotheses were developed based on the research question and a research model was proposed. Barriers and limitations which the research could face were also discussed and possible mitigations were presented.

This research extends the TTAT with the constructs subjective norm, attitude toward knowledge sharing, and experience of threat. Based on previous studies, the research investigated what effect these factors have on threat avoidance behavior. These factors determine if externalities such as social pressures or previous experiences of threat influence avoidance behavior. The literature review compiles the constructs of the proposed model, gaps in the body of knowledge, and contributions from previous studies.

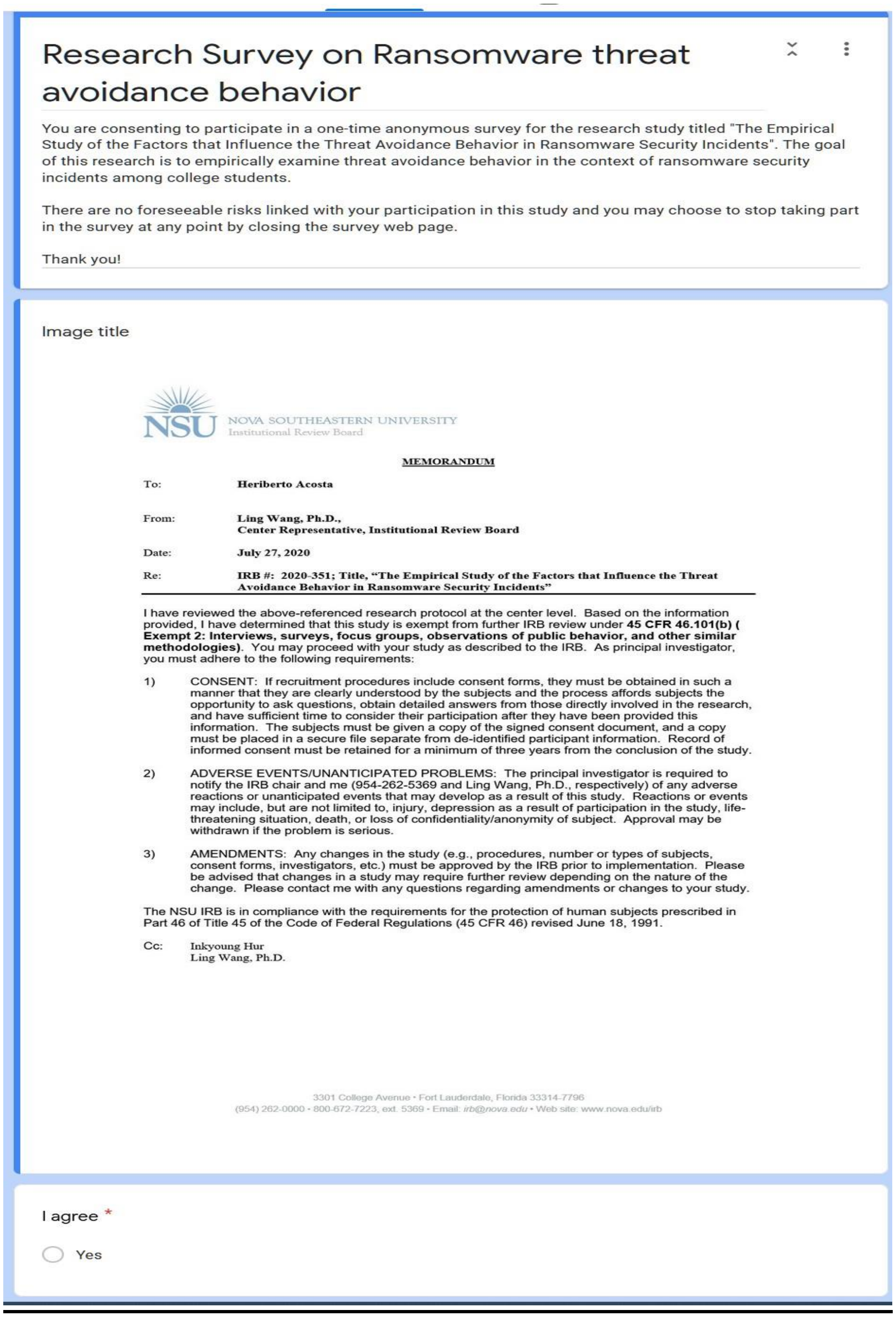
The Methodology Chapter compiles the research design. It was determined that a quantitative and empirical study using a non-probability design was the best approach for this research. The survey item was designed using the 7-point Likert Scale and the convenience sampling method was used to collect data. This chapter also discusses the design of the survey instrument, its validity and reliability, and the data collection strategy. The survey instrument was given to a panel of experts to review for clarity, application, and validation that the items measured the constructs adequately. After approval by the panel of experts, a pilot study was conducted to perform item reliability tests, determine flaws in the data collection method, and observe the possible participant response rates. Data analysis was then completed with the use of SmartPLS 3.0 and SPSS. These statistical and modeling tools were used to test for factor analysis, construct reliability and validity, measurement model, and structural model. The results and analyses of these tests were presented in Chapter 4 and the Appendices. The analysis of the statistical results was then used to reject or support the hypotheses. Chapter 5 presents the study conclusions, the implications and recommendations, limitations, and possible future research.

The study brought into focus a particular sector of user that is not usually studied, college students. The results provide a better understanding of college students' threat avoidance behavior in the face of ransomware infections. It also concluded with unexpected results. Some of the hypotheses were not supported as was expected based on previous literature. Future studies should focus on why the results of previous studies in other population demographics and sectors were so different when applied in the context of college students. Also, the results provided insight into the technical experience students have, their knowledge of university IT security policies, and differences among computing and non-computing students. The results of the study shed light on an important population that is not studied enough in the context of ransomware attacks and how they respond or act to prevent the infections. It is interesting that some results were opposite to what is seen in studies done in the corporate environment. Also, it cannot be ignored that the stresses affecting students since March 2020 due to the Covid-19 pandemic may have affected their answers. More studies should be made to better understand how subjective norm affects a lesser experienced population and its relationship with attitude toward knowledge sharing after the pandemic is under control and students go back to the normal daily circumstances. Finally, further study is necessary to determine why the experience of threat did not have the expected strong effect on perceived threat and if this may have to do with the impulsivity and risk taking tendencies of the demographic under question.

Appendices

Appendix A

Survey Questionnaire



Research Survey on Ransomware threat avoidance behavior

You are consenting to participate in a one-time anonymous survey for the research study titled "The Empirical Study of the Factors that Influence the Threat Avoidance Behavior in Ransomware Security Incidents". The goal of this research is to empirically examine threat avoidance behavior in the context of ransomware security incidents among college students.

There are no foreseeable risks linked with your participation in this study and you may choose to stop taking part in the survey at any point by closing the survey web page.

Thank you!

Image title

NSU NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **Heriberto Acosta**

From: **Ling Wang, Ph.D.,**
Center Representative, Institutional Review Board

Date: **July 27, 2020**

Re: **IRB #: 2020-351; Title, "The Empirical Study of the Factors that Influence the Threat Avoidance Behavior in Ransomware Security Incidents"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

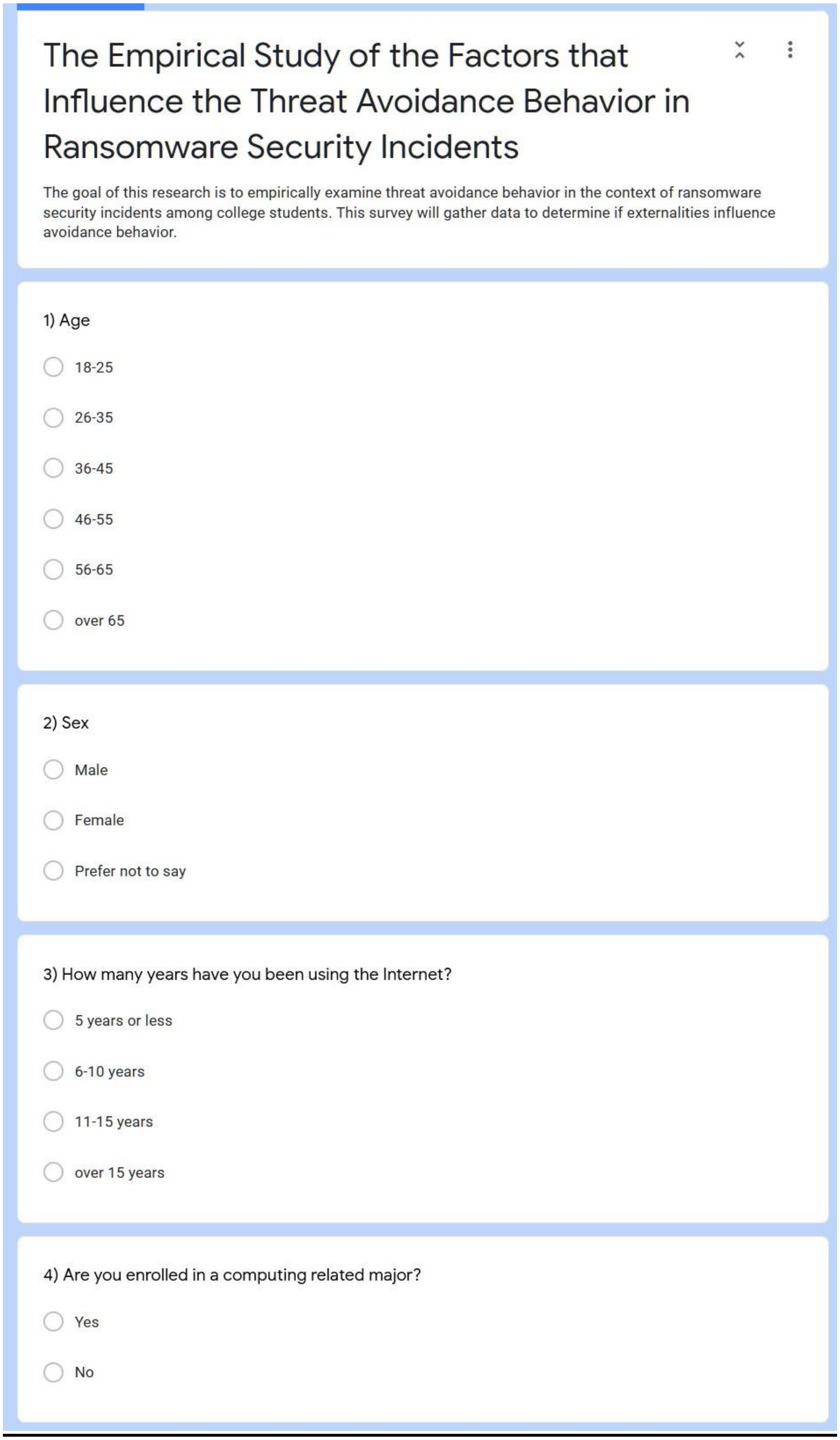
The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Inkyoung Hur
Ling Wang, Ph.D.

3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-0000 • 800-672-7223, ext. 5369 • Email: *irb@nova.edu* • Web site: www.nova.edu/irb

I agree *

○ Yes



The Empirical Study of the Factors that Influence the Threat Avoidance Behavior in Ransomware Security Incidents

The goal of this research is to empirically examine threat avoidance behavior in the context of ransomware security incidents among college students. This survey will gather data to determine if externalities influence avoidance behavior.

1) Age

○ 18-25

○ 26-35

○ 36-45

○ 46-55

○ 56-65

○ over 65

2) Sex

○ Male

○ Female

○ Prefer not to say

3) How many years have you been using the Internet?

○ 5 years or less

○ 6-10 years

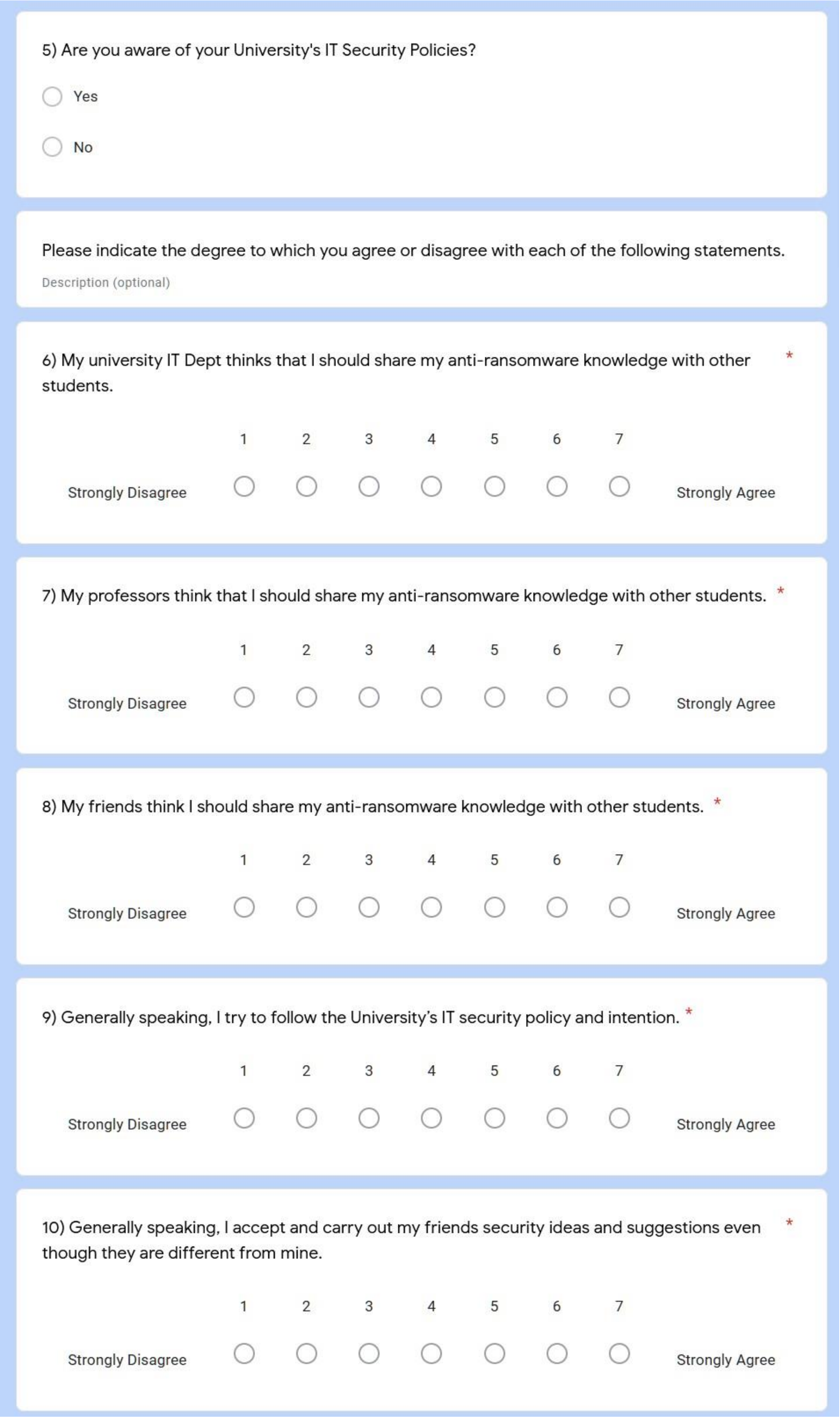
○ 11-15 years

○ over 15 years

4) Are you enrolled in a computing related major?

○ Yes

○ No



5) Are you aware of your University's IT Security Policies?

○ Yes

○ No

Please indicate the degree to which you agree or disagree with each of the following statements.

Description (optional)

6) My university IT Dept thinks that I should share my anti-ransomware knowledge with other students. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

7) My professors think that I should share my anti-ransomware knowledge with other students. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

8) My friends think I should share my anti-ransomware knowledge with other students. *

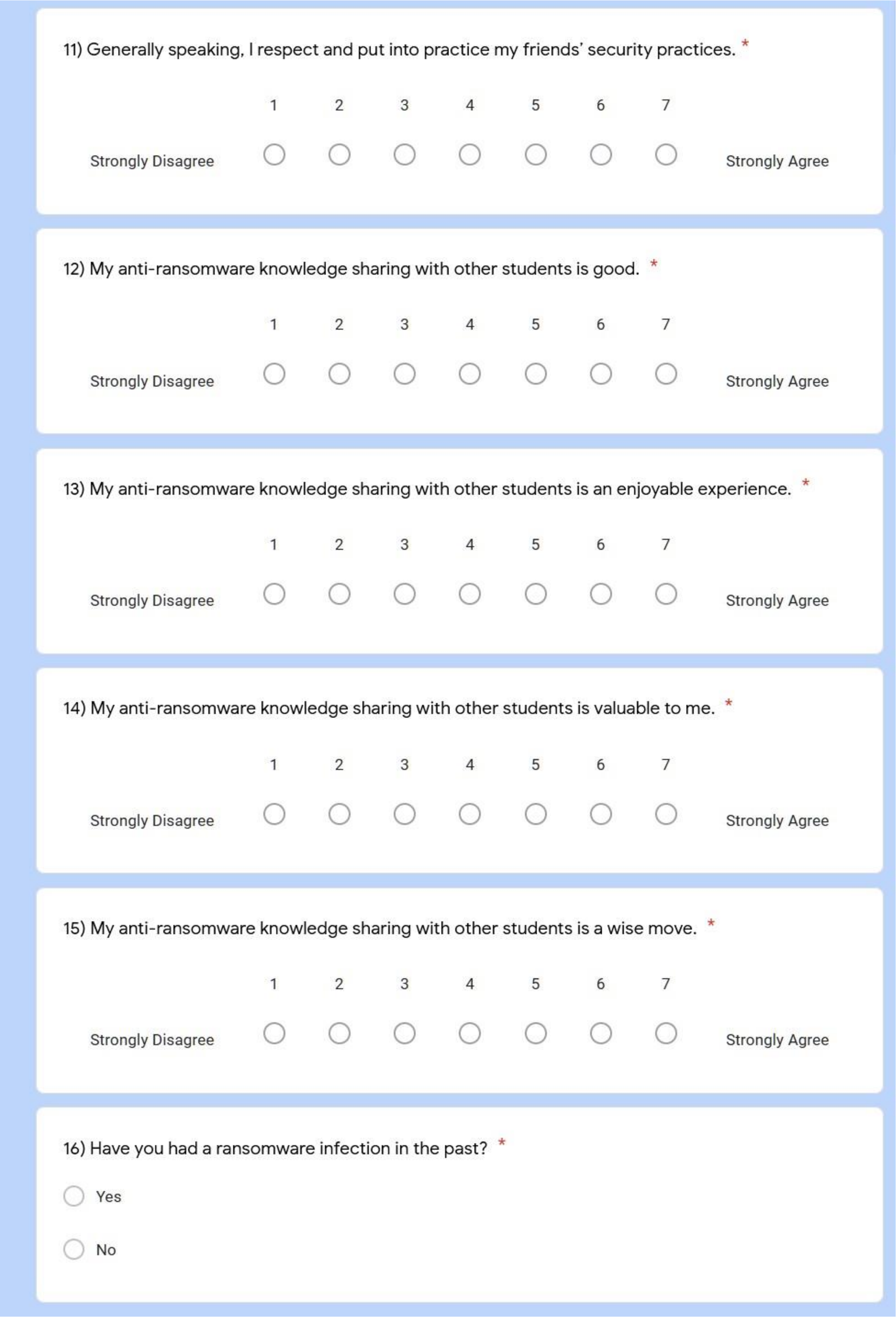
	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

9) Generally speaking, I try to follow the University's IT security policy and intention. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

10) Generally speaking, I accept and carry out my friends security ideas and suggestions even though they are different from mine. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree



11) Generally speaking, I respect and put into practice my friends' security practices. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

12) My anti-ransomware knowledge sharing with other students is good. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

13) My anti-ransomware knowledge sharing with other students is an enjoyable experience. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

14) My anti-ransomware knowledge sharing with other students is valuable to me. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

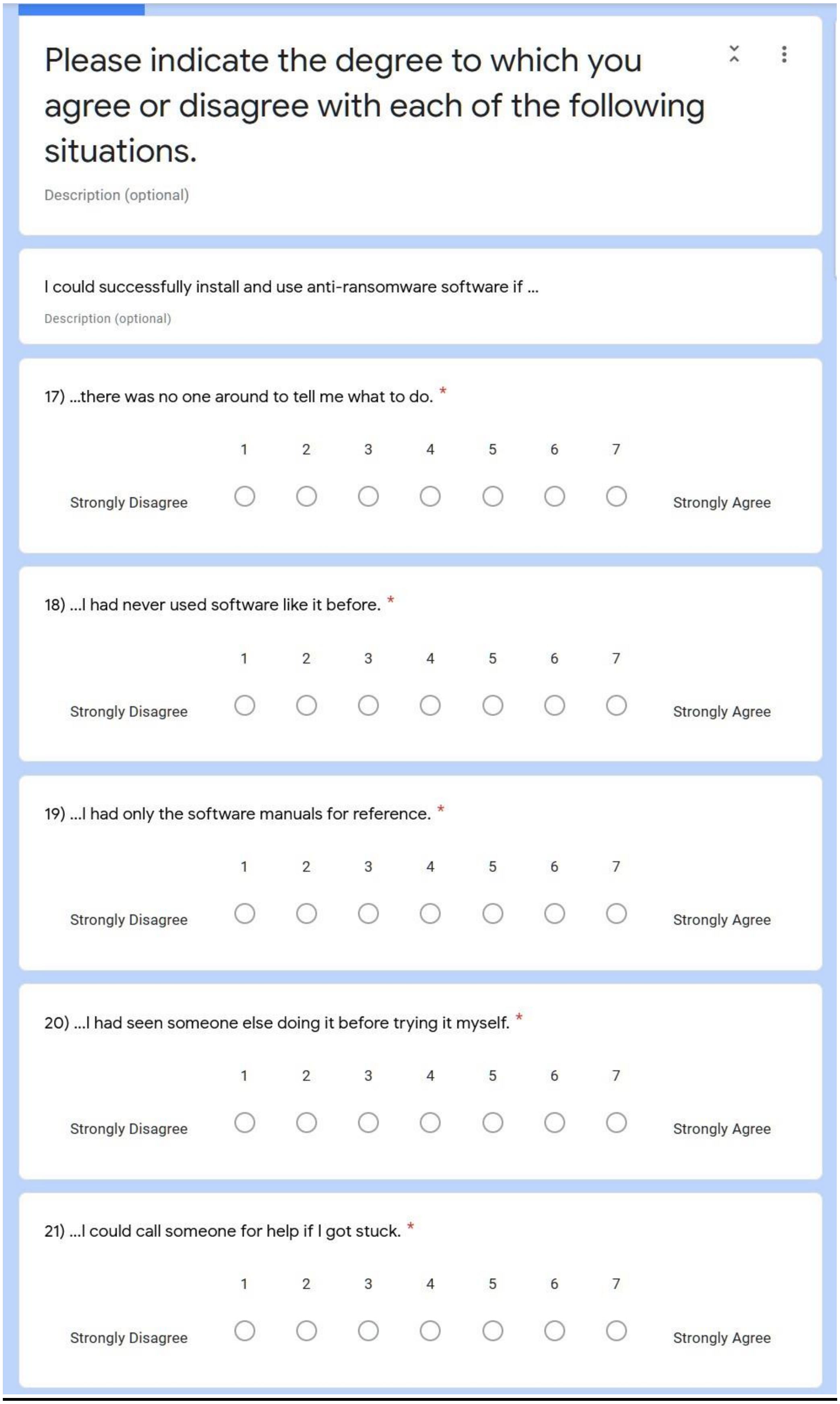
15) My anti-ransomware knowledge sharing with other students is a wise move. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

16) Have you had a ransomware infection in the past? *

○ Yes

○ No



Please indicate the degree to which you agree or disagree with each of the following situations.

Description (optional)

I could successfully install and use anti-ransomware software if ...

Description (optional)

17) ...there was no one around to tell me what to do. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

18) ...I had never used software like it before. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

19) ...I had only the software manuals for reference. *

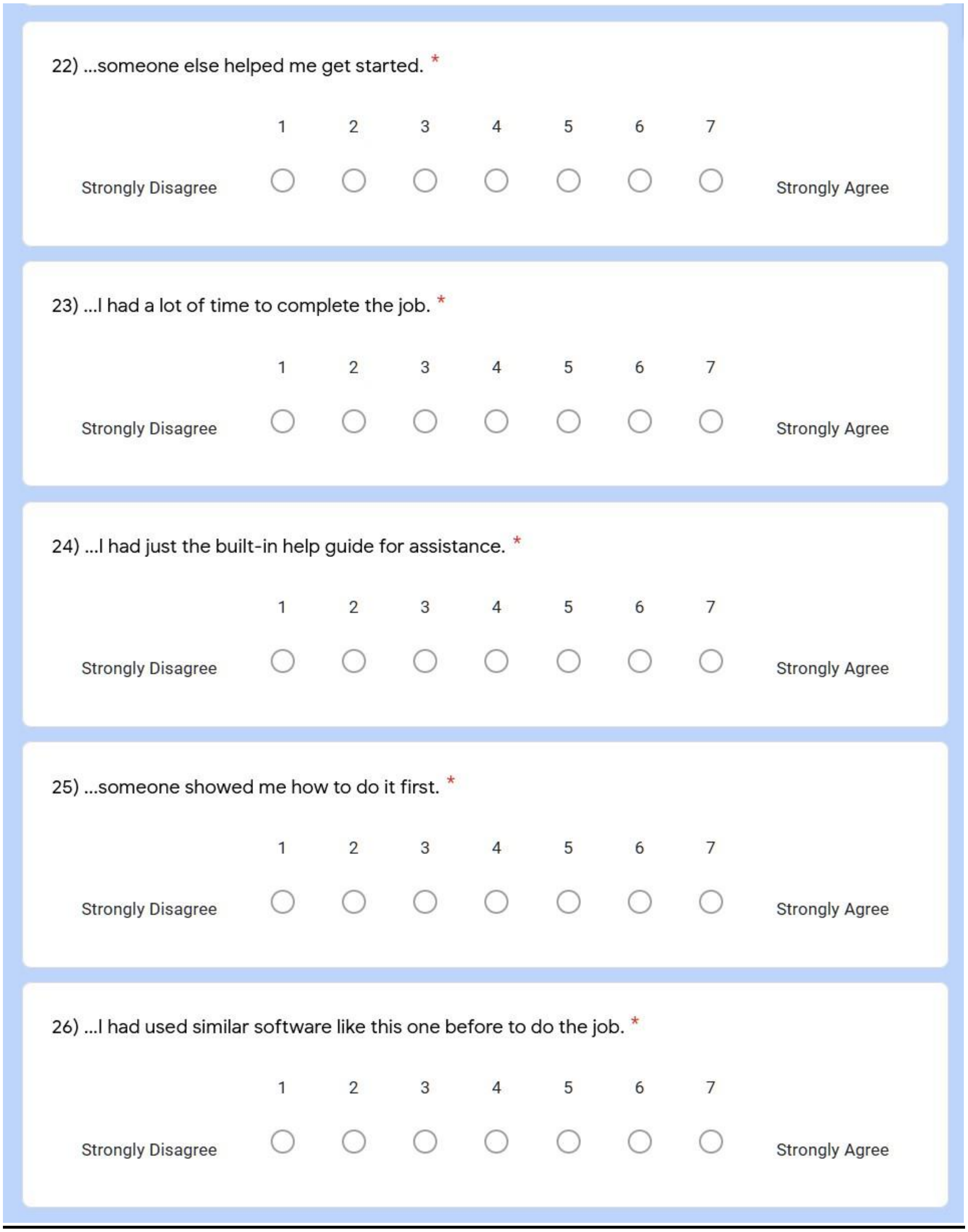
	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

20) ...I had seen someone else doing it before trying it myself. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

21) ...I could call someone for help if I got stuck. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree



22) ...someone else helped me get started. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

23) ...I had a lot of time to complete the job. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

24) ...I had just the built-in help guide for assistance. *

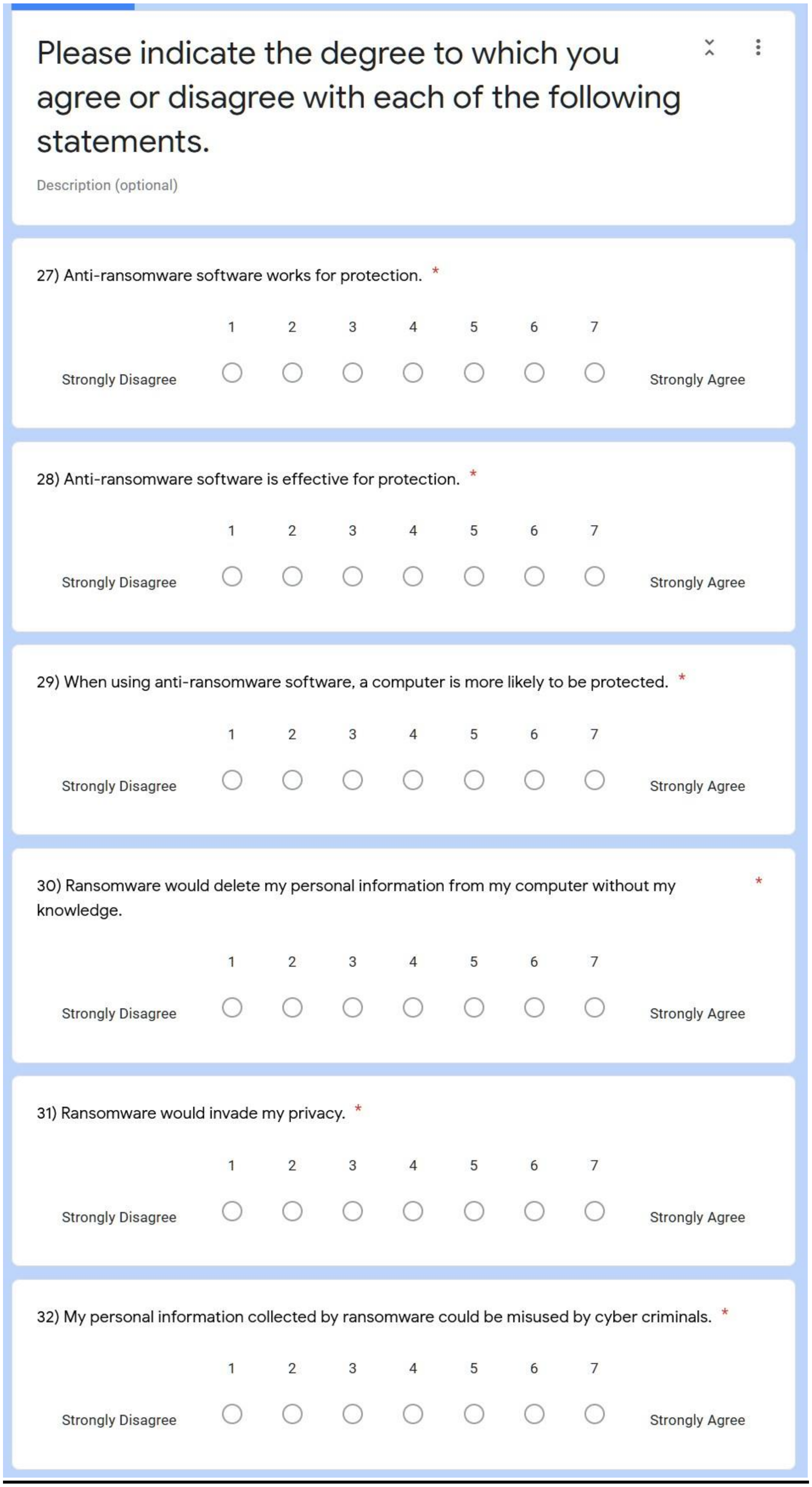
	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

25) ...someone showed me how to do it first. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

26) ...I had used similar software like this one before to do the job. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree



Please indicate the degree to which you agree or disagree with each of the following statements.

Description (optional)

27) Anti-ransomware software works for protection. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

28) Anti-ransomware software is effective for protection. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

29) When using anti-ransomware software, a computer is more likely to be protected. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

30) Ransomware would delete my personal information from my computer without my knowledge. *

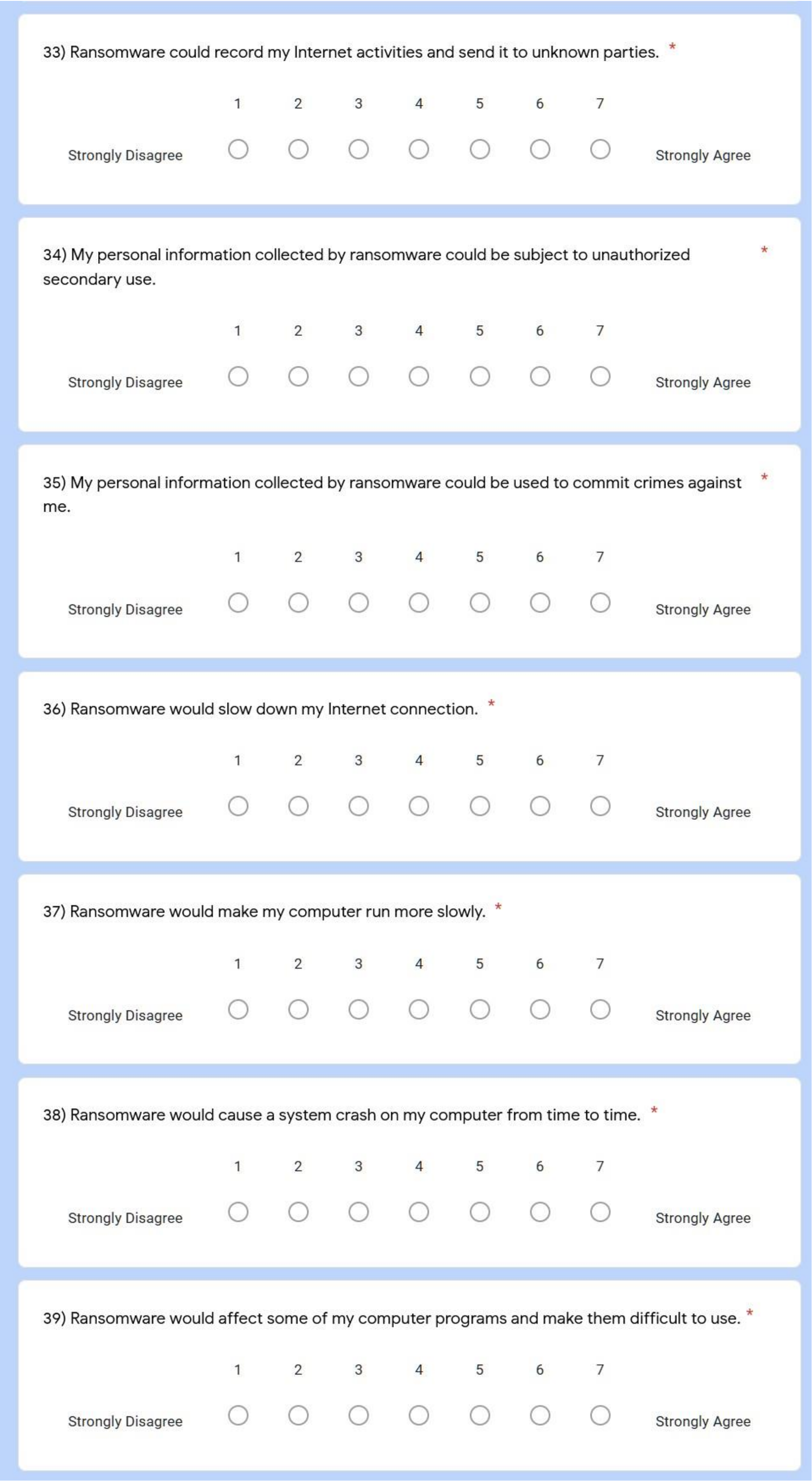
	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

31) Ransomware would invade my privacy. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

32) My personal information collected by ransomware could be misused by cyber criminals. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree



33) Ransomware could record my Internet activities and send it to unknown parties. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

34) My personal information collected by ransomware could be subject to unauthorized secondary use. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

35) My personal information collected by ransomware could be used to commit crimes against me. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

36) Ransomware would slow down my Internet connection. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

37) Ransomware would make my computer run more slowly. *

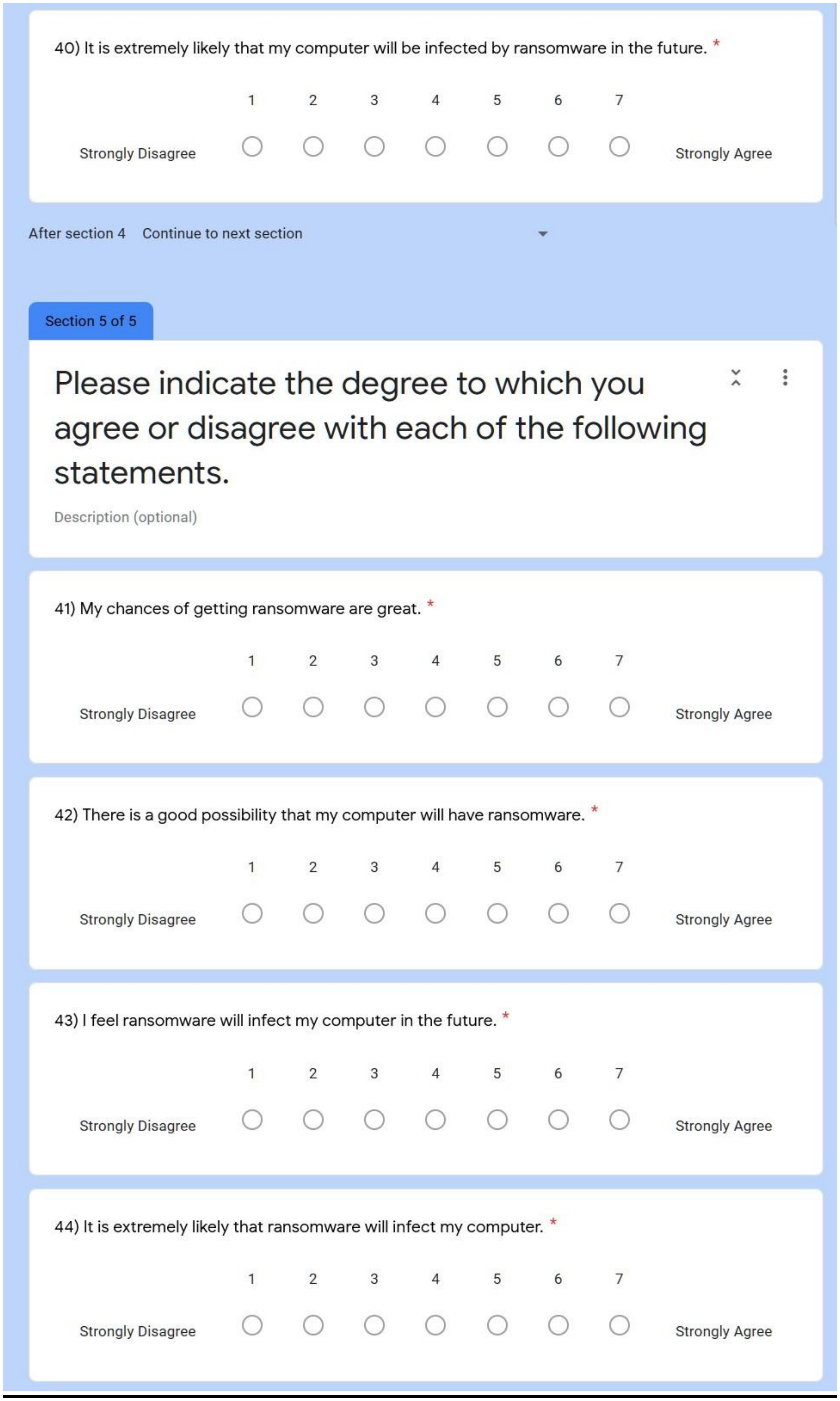
	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

38) Ransomware would cause a system crash on my computer from time to time. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

39) Ransomware would affect some of my computer programs and make them difficult to use. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree



40) It is extremely likely that my computer will be infected by ransomware in the future. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

After section 4 Continue to next section

Section 5 of 5

Please indicate the degree to which you agree or disagree with each of the following statements.

Description (optional)

41) My chances of getting ransomware are great. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

42) There is a good possibility that my computer will have ransomware. *

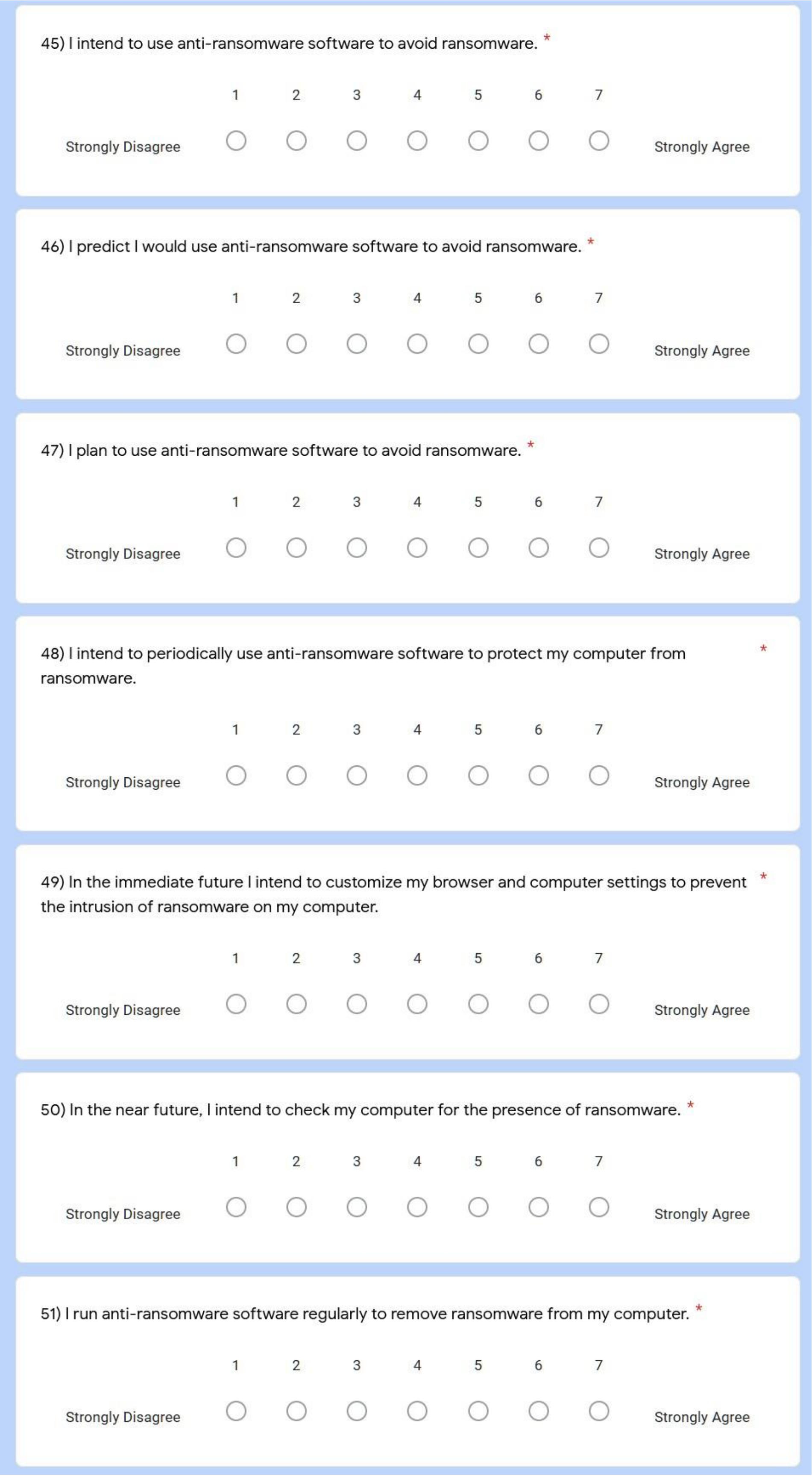
	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

43) I feel ransomware will infect my computer in the future. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

44) It is extremely likely that ransomware will infect my computer. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree



45) I intend to use anti-ransomware software to avoid ransomware. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

46) I predict I would use anti-ransomware software to avoid ransomware. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

47) I plan to use anti-ransomware software to avoid ransomware. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

48) I intend to periodically use anti-ransomware software to protect my computer from ransomware. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

49) In the immediate future I intend to customize my browser and computer settings to prevent the intrusion of ransomware on my computer. *

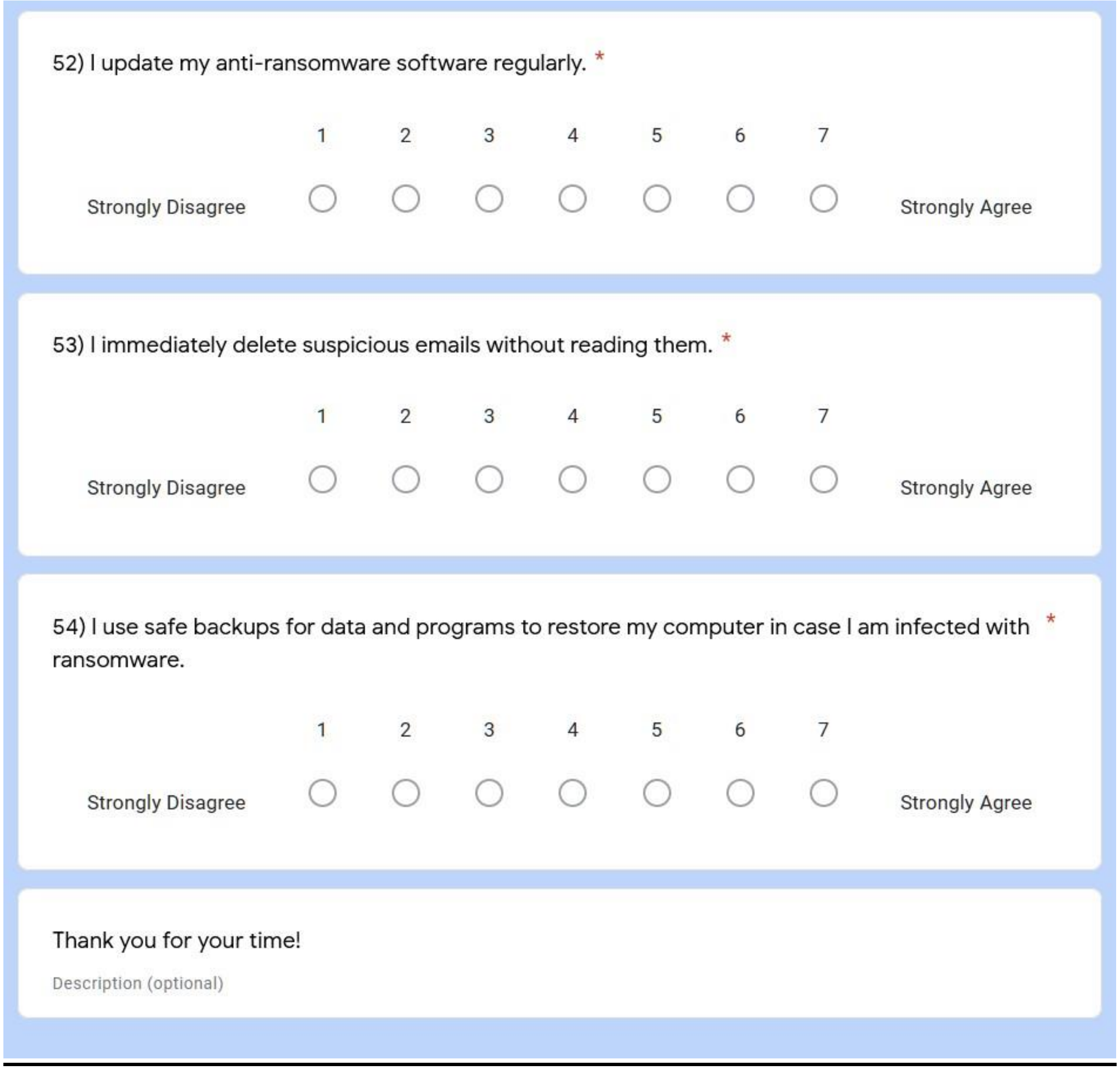
	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

50) In the near future, I intend to check my computer for the presence of ransomware. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

51) I run anti-ransomware software regularly to remove ransomware from my computer. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree



52) I update my anti-ransomware software regularly. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

53) I immediately delete suspicious emails without reading them. *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

54) I use safe backups for data and programs to restore my computer in case I am infected with ransomware. *

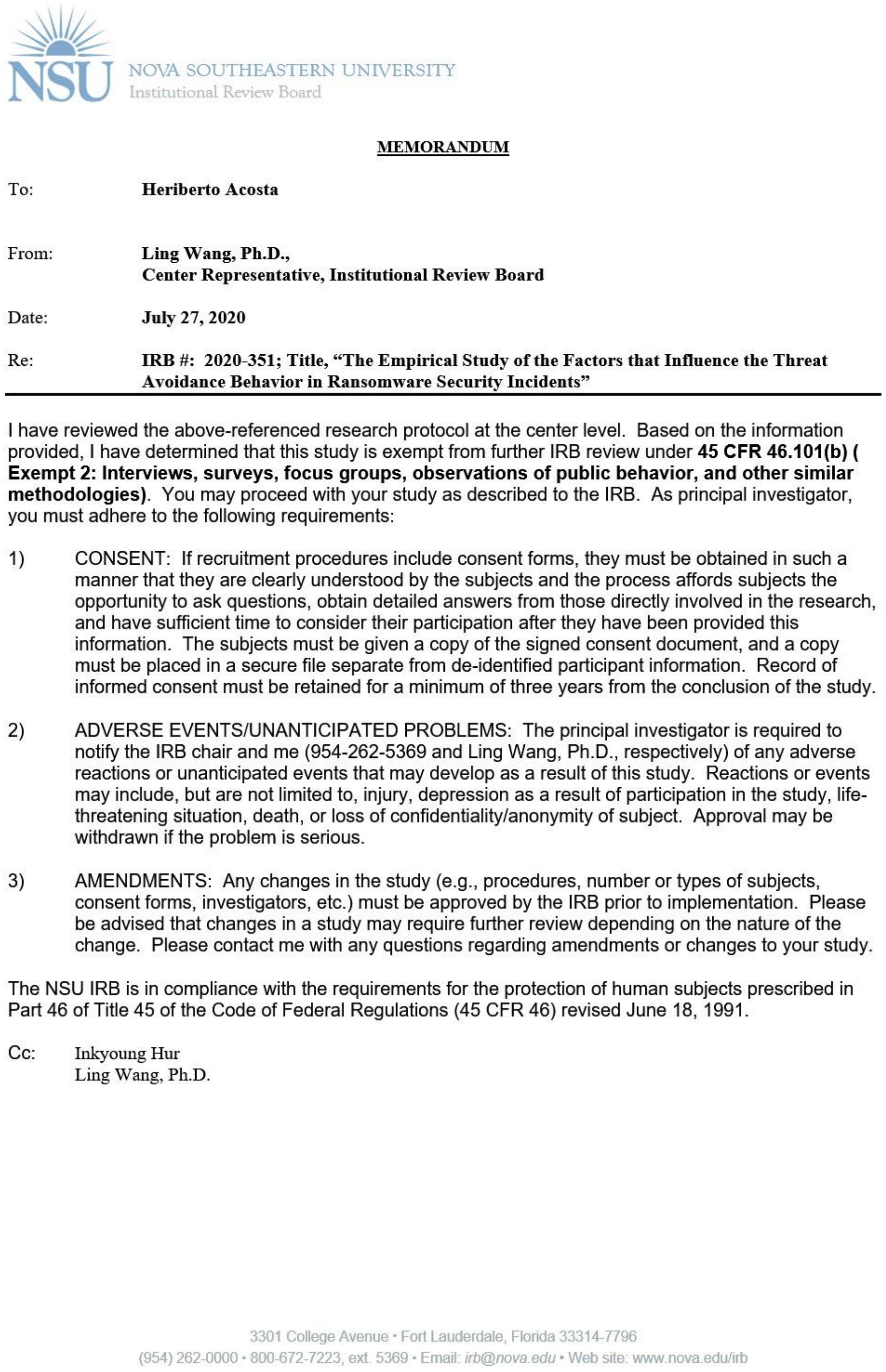
	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

Thank you for your time!

Description (optional)

Appendix B

IRB Approval Letter



NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **Heriberto Acosta**

From: **Ling Wang, Ph.D.,**
Center Representative, Institutional Review Board

Date: **July 27, 2020**

Re: **IRB #: 2020-351; Title, "The Empirical Study of the Factors that Influence the Threat Avoidance Behavior in Ransomware Security Incidents"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Inkyoung Hur
Ling Wang, Ph.D.

3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-0000 • 800-672-7223, ext. 5369 • Email: *irb@nova.edu* • Web site: www.nova.edu/irb

Appendix C

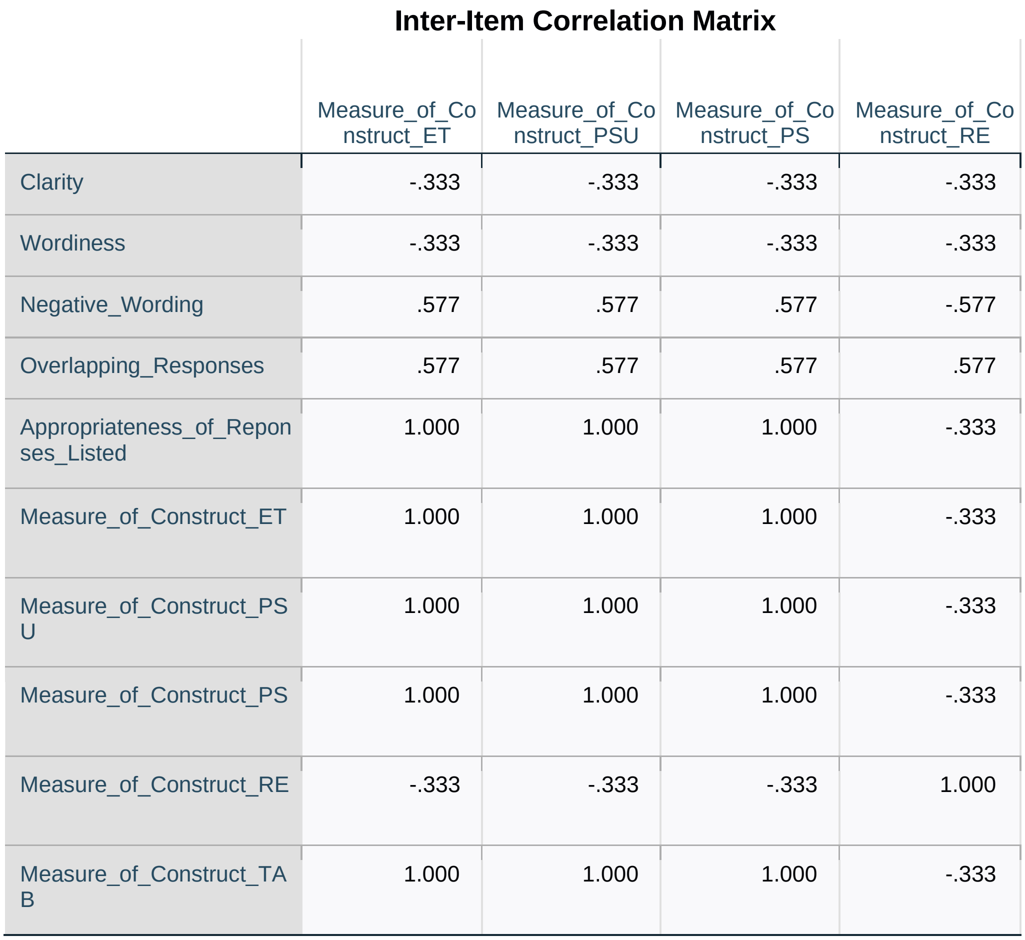
Pilot Study Expert Panel Reliability Statistics

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.707	.708	10

Inter-Item Correlation Matrix

	Clarity	Wordiness	Negative_Wording	Overlapping_Responses	Appropriateness_of_Reponses_Listed
Clarity	1.000	1.000	-.577	-.577	-.333
Wordiness	1.000	1.000	-.577	-.577	-.333
Negative_Wording	-.577	-.577	1.000	.000	.577
Overlapping_Responses	-.577	-.577	.000	1.000	.577
Appropriateness_of_Repon ses_Listed	-.333	-.333	.577	.577	1.000
Measure_of_Construct_ET	-.333	-.333	.577	.577	1.000
Measure_of_Construct_PSU	-.333	-.333	.577	.577	1.000
Measure_of_Construct_PS	-.333	-.333	.577	.577	1.000
Measure_of_Construct_RE	-.333	-.333	-.577	.577	-.333
Measure_of_Construct_TAB	-.333	-.333	.577	.577	1.000

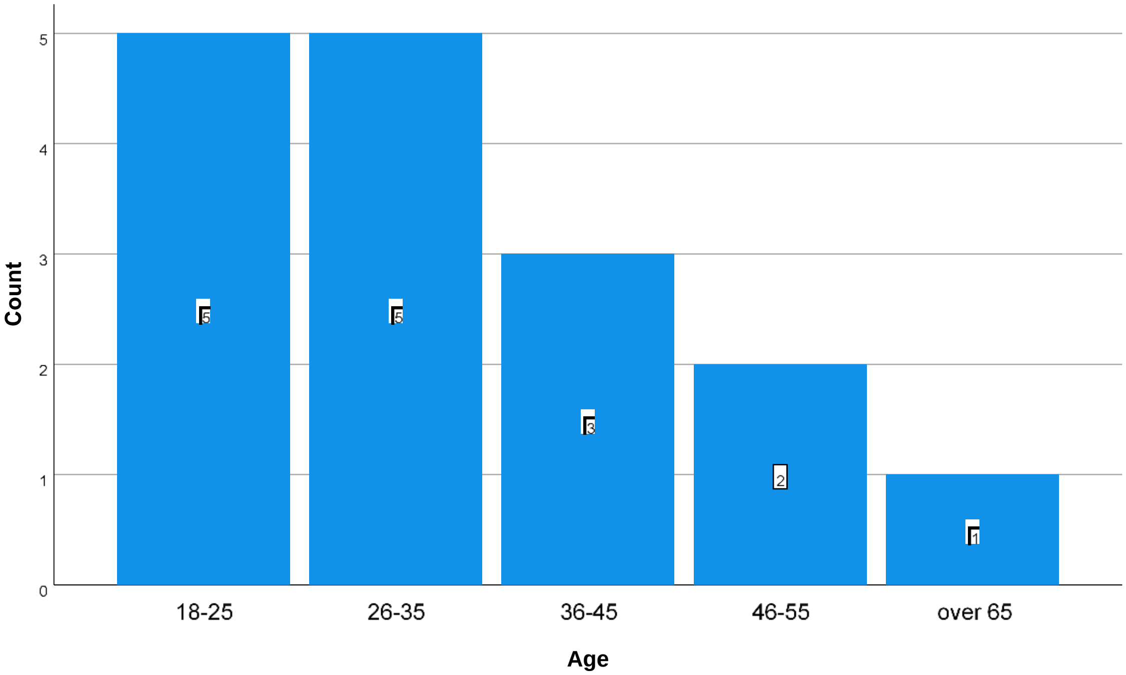


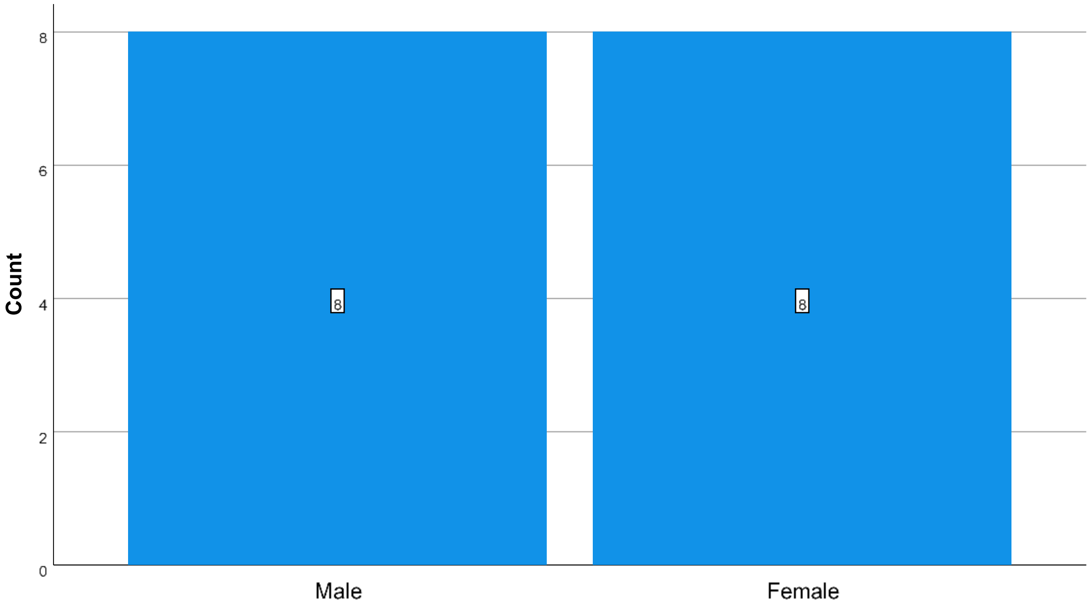
Inter-Item Correlation Matrix

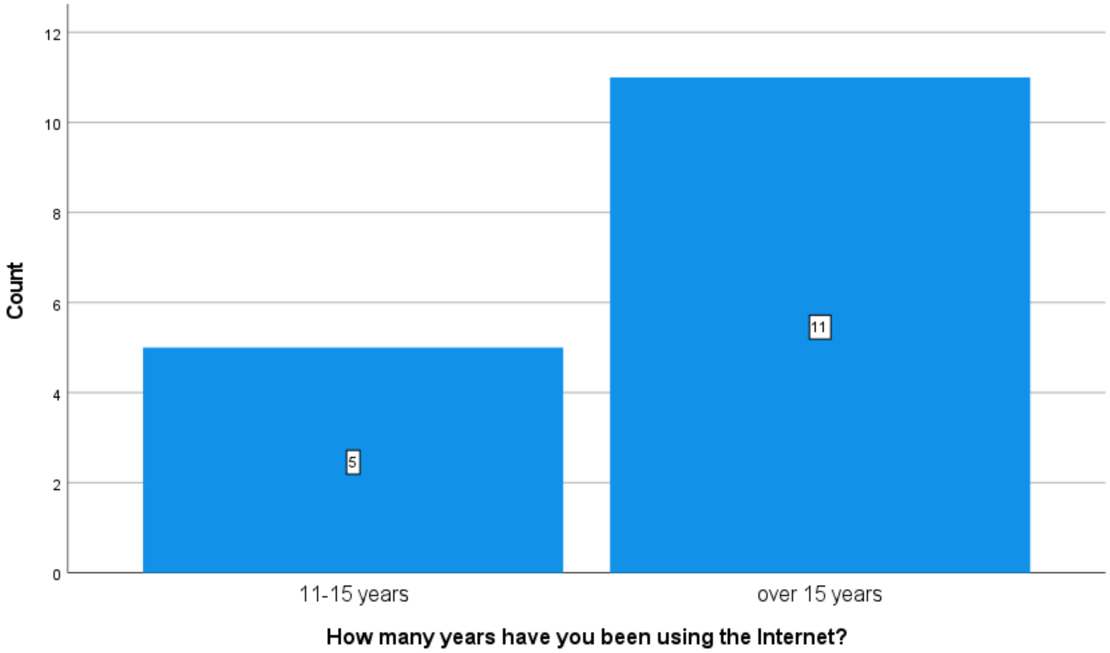
	Measure_of_Construct_ET	Measure_of_Construct_PSU	Measure_of_Construct_PS	Measure_of_Construct_RE
Clarity	-.333	-.333	-.333	-.333
Wordiness	-.333	-.333	-.333	-.333
Negative_Wording	.577	.577	.577	-.577
Overlapping_Responses	.577	.577	.577	.577
Appropriateness_of_Reponses_Listed	1.000	1.000	1.000	-.333
Measure_of_Construct_ET	1.000	1.000	1.000	-.333
Measure_of_Construct_PSU	1.000	1.000	1.000	-.333
Measure_of_Construct_PS	1.000	1.000	1.000	-.333
Measure_of_Construct_RE	-.333	-.333	-.333	1.000
Measure_of_Construct_TAB	1.000	1.000	1.000	-.333

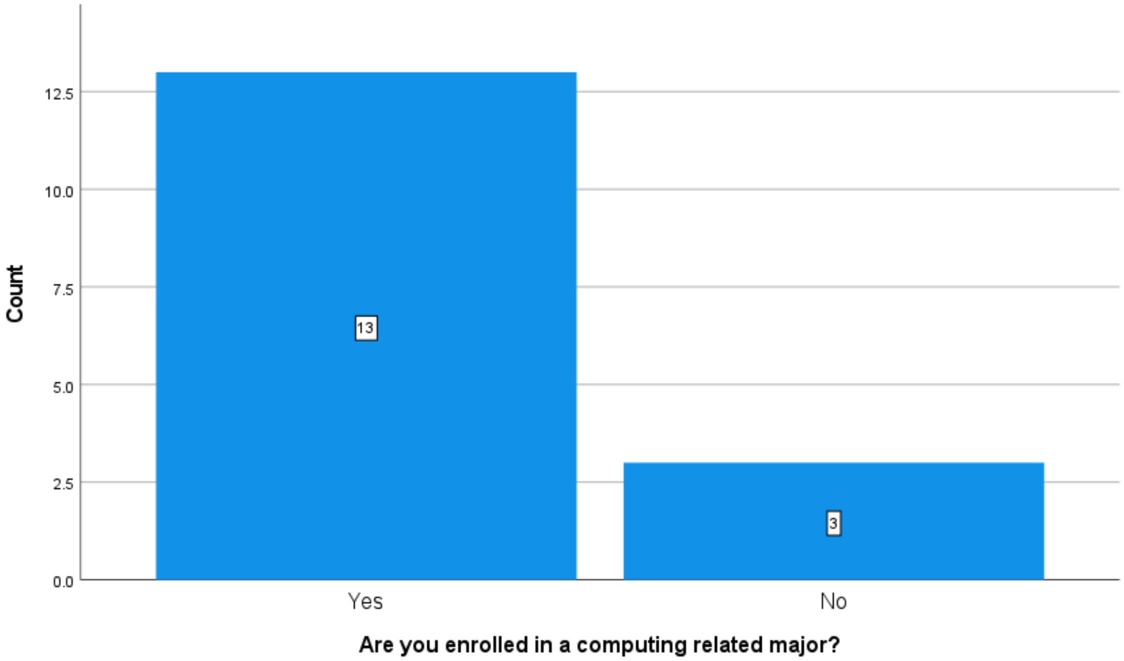
Appendix D

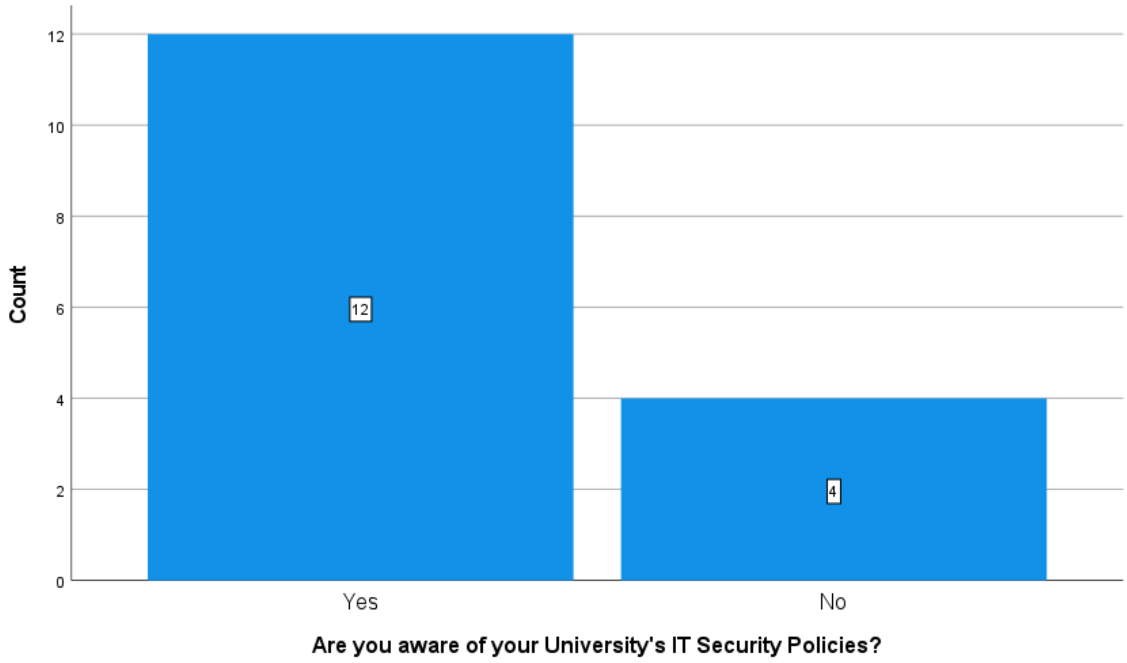
Pilot Study Descriptive and Reliability Statistics

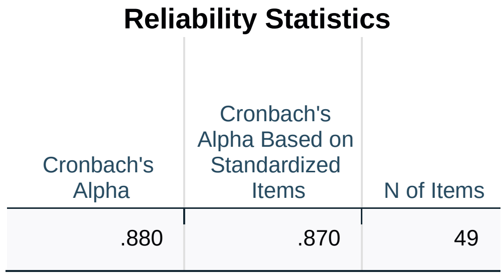





Count
12
10
8
6
4
2
0
5
11
11-15 years
over 15 years
How many years have you been using the Internet?

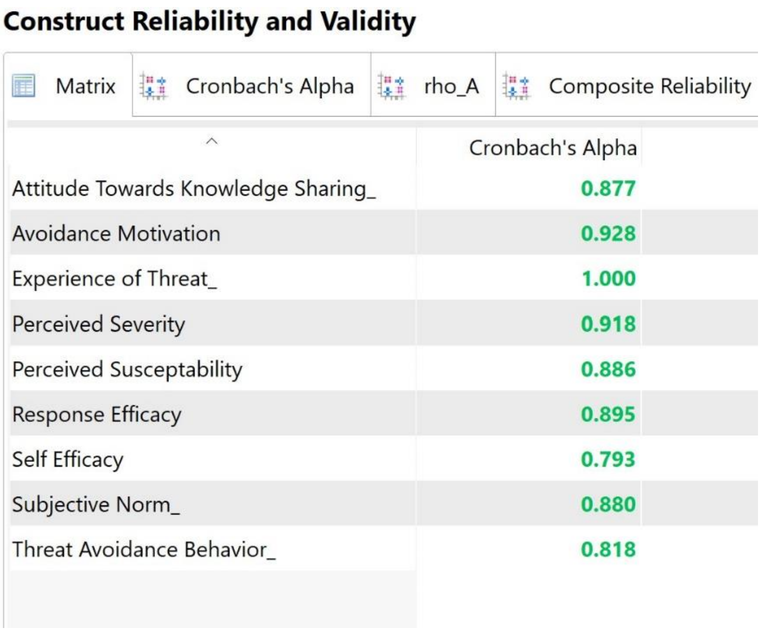

Count
12.5
10.0
7.5
5.0
2.5
0.0
13
3
Yes
No
Are you enrolled in a computing related major?





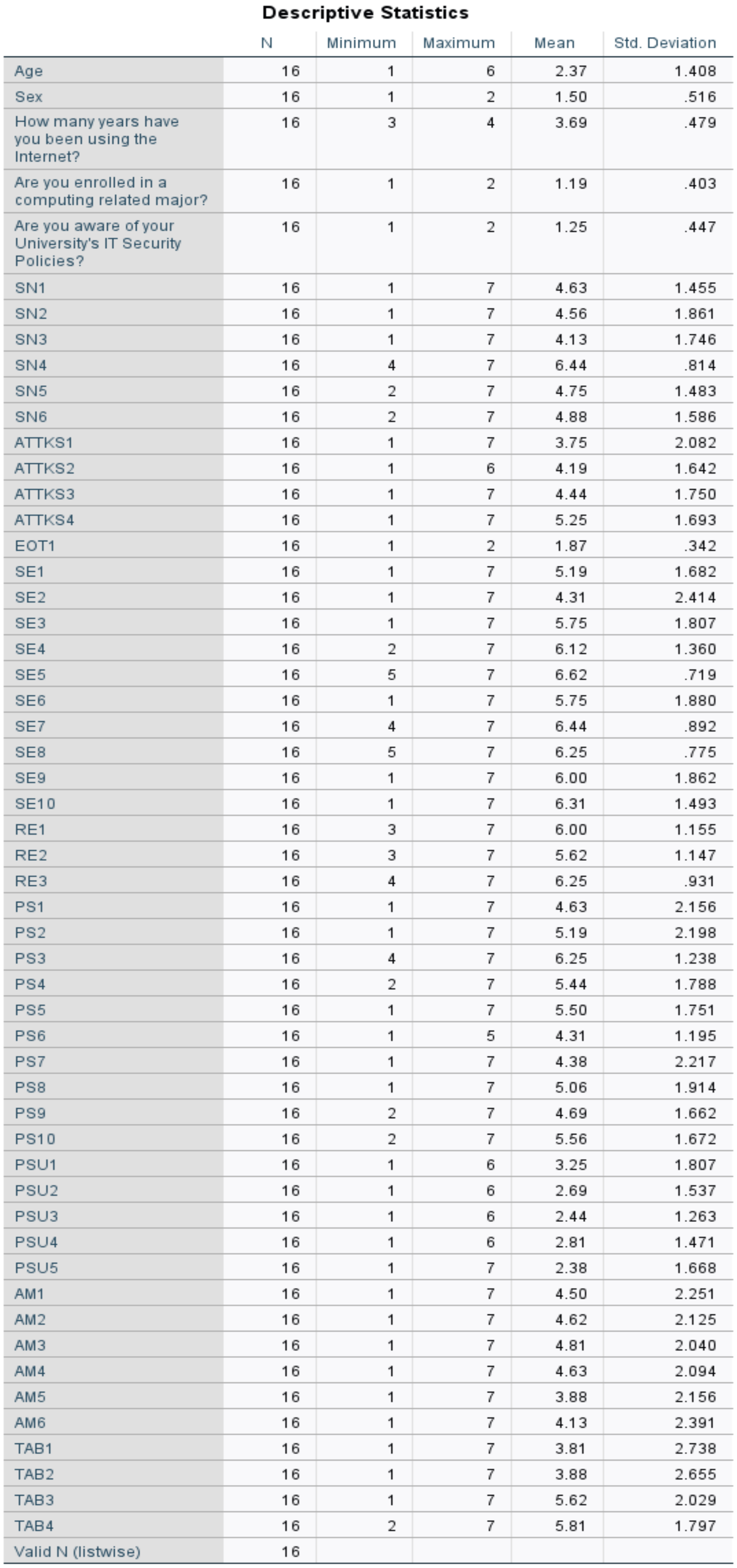
Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.880	.870	49



Construct Reliability and Validity

	Cronbach's Alpha
Attitude Towards Knowledge Sharing_	0.877
Avoidance Motivation	0.928
Experience of Threat_	1.000
Perceived Severity	0.918
Perceived Susceptability	0.886
Response Efficacy	0.895
Self Efficacy	0.793
Subjective Norm_	0.880
Threat Avoidance Behavior_	0.818

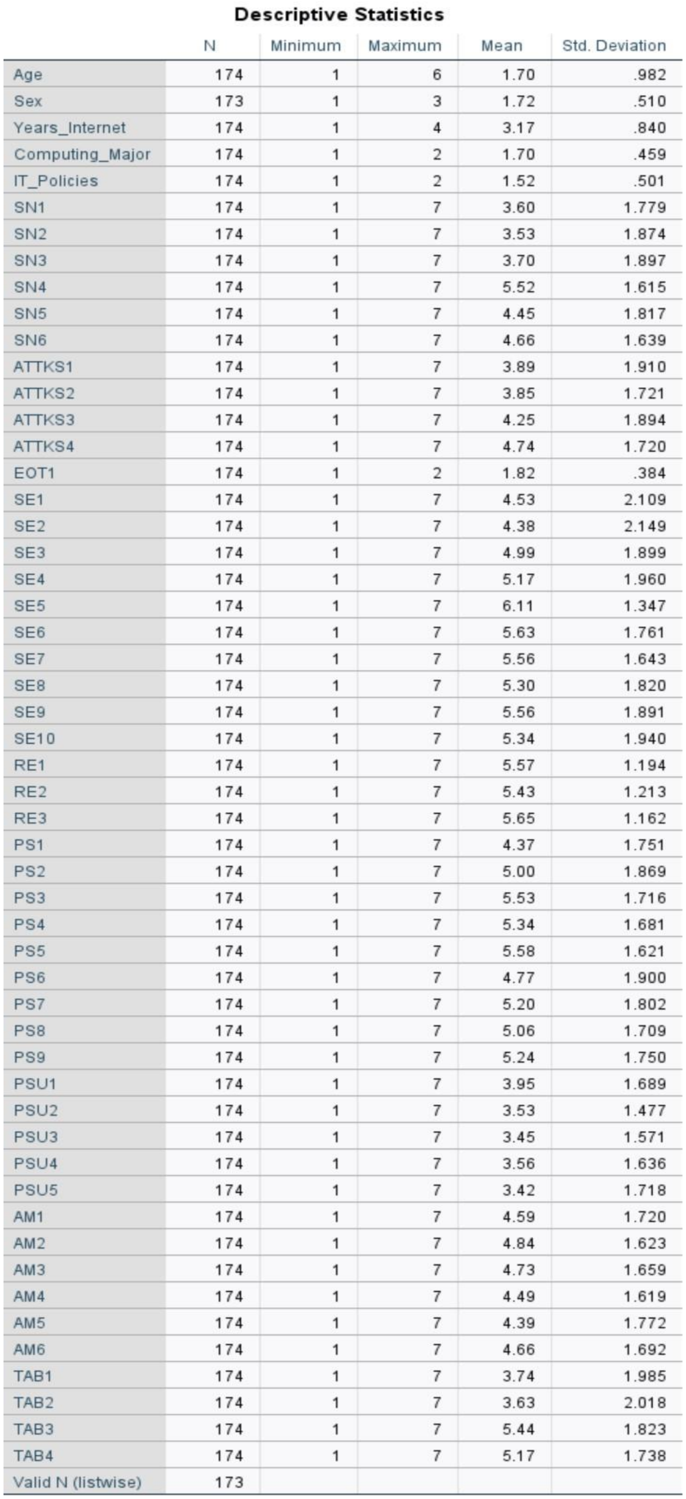


Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Age	16	1	6	2.37	1.408
Sex	16	1	2	1.50	.516
How many years have you been using the Internet?	16	3	4	3.69	.479
Are you enrolled in a computing related major?	16	1	2	1.19	.403
Are you aware of your University's IT Security Policies?	16	1	2	1.25	.447
SN1	16	1	7	4.63	1.455
SN2	16	1	7	4.56	1.861
SN3	16	1	7	4.13	1.746
SN4	16	4	7	6.44	.814
SN5	16	2	7	4.75	1.483
SN6	16	2	7	4.88	1.586
ATTKS1	16	1	7	3.75	2.082
ATTKS2	16	1	6	4.19	1.642
ATTKS3	16	1	7	4.44	1.750
ATTKS4	16	1	7	5.25	1.693
EOT1	16	1	2	1.87	.342
SE1	16	1	7	5.19	1.682
SE2	16	1	7	4.31	2.414
SE3	16	1	7	5.75	1.807
SE4	16	2	7	6.12	1.360
SE5	16	5	7	6.62	.719
SE6	16	1	7	5.75	1.880
SE7	16	4	7	6.44	.892
SE8	16	5	7	6.25	.775
SE9	16	1	7	6.00	1.862
SE10	16	1	7	6.31	1.493
RE1	16	3	7	6.00	1.155
RE2	16	3	7	5.62	1.147
RE3	16	4	7	6.25	.931
PS1	16	1	7	4.63	2.156
PS2	16	1	7	5.19	2.198
PS3	16	4	7	6.25	1.238
PS4	16	2	7	5.44	1.788
PS5	16	1	7	5.50	1.751
PS6	16	1	5	4.31	1.195
PS7	16	1	7	4.38	2.217
PS8	16	1	7	5.06	1.914
PS9	16	2	7	4.69	1.662
PS10	16	2	7	5.56	1.672
PSU1	16	1	6	3.25	1.807
PSU2	16	1	6	2.69	1.537
PSU3	16	1	6	2.44	1.263
PSU4	16	1	6	2.81	1.471
PSU5	16	1	7	2.38	1.668
AM1	16	1	7	4.50	2.251
AM2	16	1	7	4.62	2.125
AM3	16	1	7	4.81	2.040
AM4	16	1	7	4.63	2.094
AM5	16	1	7	3.88	2.156
AM6	16	1	7	4.13	2.391
TAB1	16	1	7	3.81	2.738
TAB2	16	1	7	3.88	2.655
TAB3	16	1	7	5.62	2.029
TAB4	16	2	7	5.81	1.797
Valid N (listwise)	16				

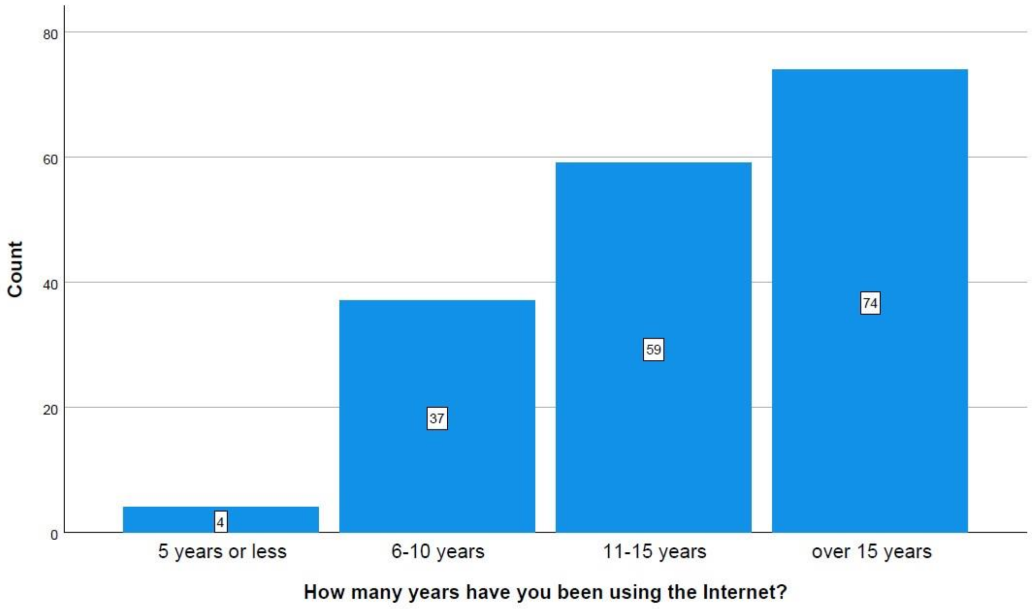
Appendix E

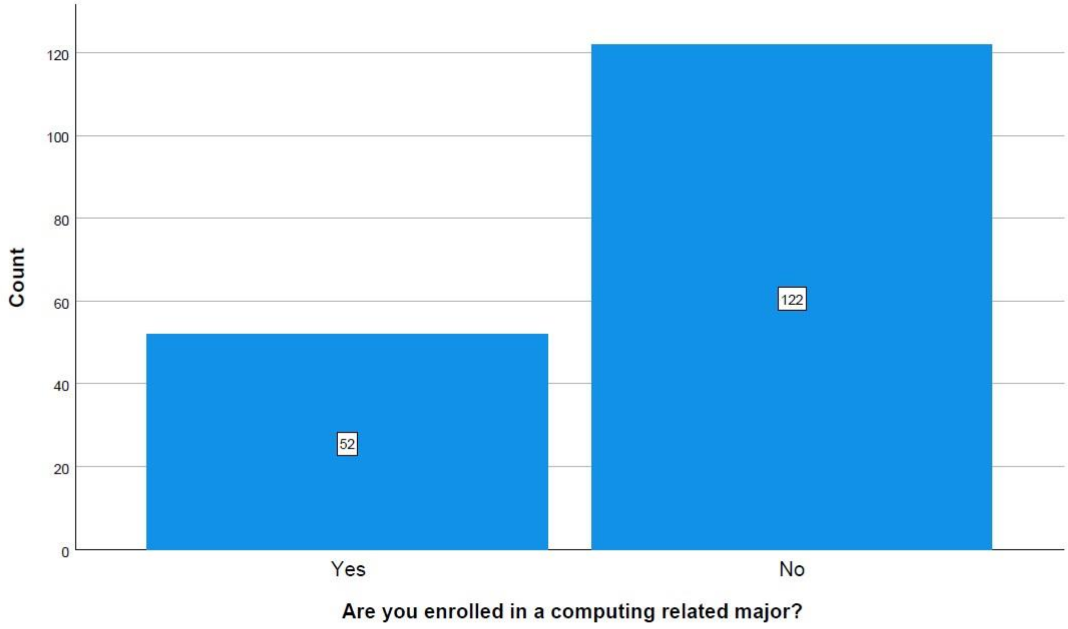
Main Study Pre-Analysis Statistics

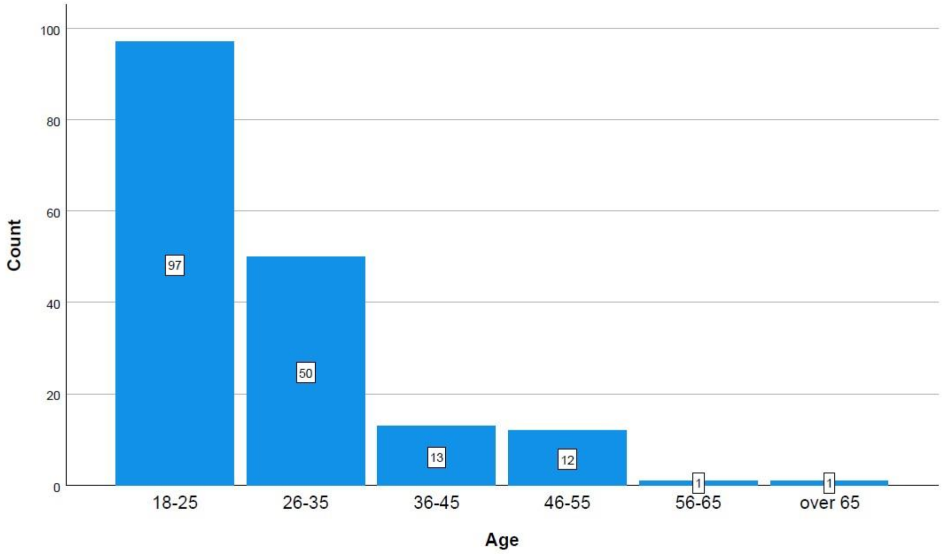


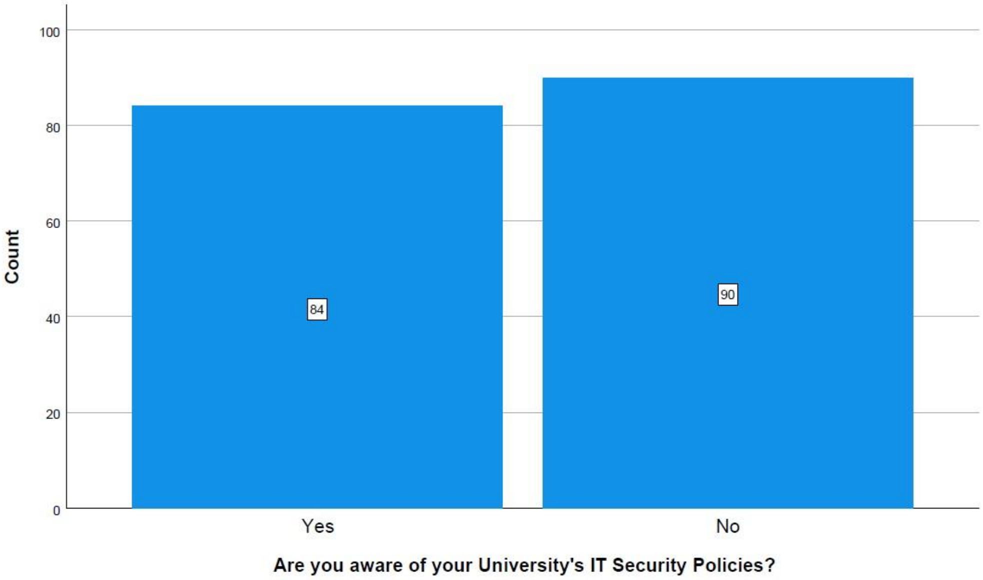
Descriptive Statistics

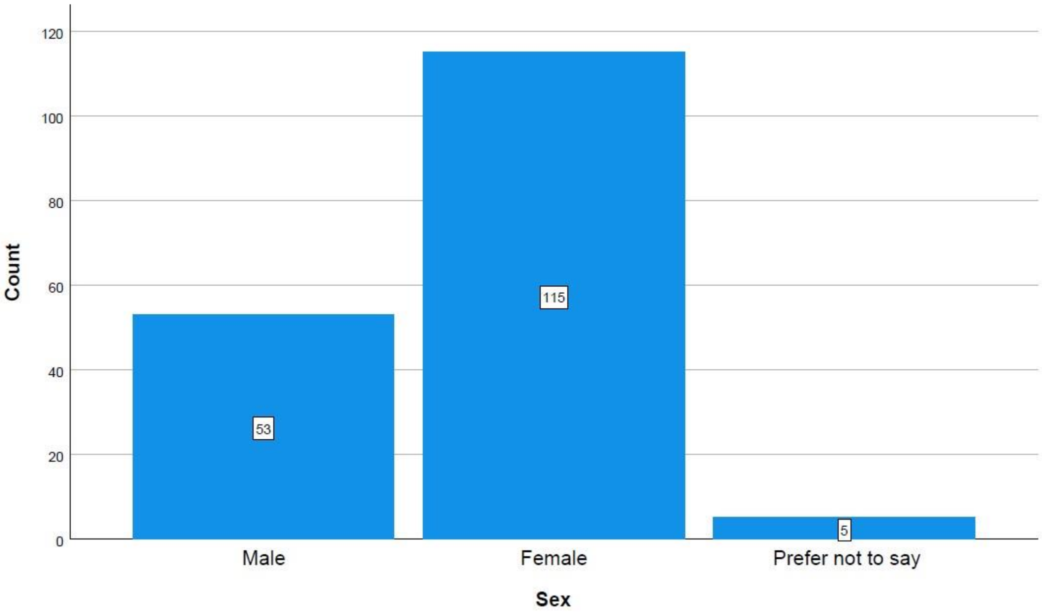
	N	Minimum	Maximum	Mean	Std. Deviation
Age	174	1	6	1.70	.982
Sex	173	1	3	1.72	.510
Years_Internet	174	1	4	3.17	.840
Computing_Major	174	1	2	1.70	.459
IT_Policies	174	1	2	1.52	.501
SN1	174	1	7	3.60	1.779
SN2	174	1	7	3.53	1.874
SN3	174	1	7	3.70	1.897
SN4	174	1	7	5.52	1.615
SN5	174	1	7	4.45	1.817
SN6	174	1	7	4.66	1.639
ATTKS1	174	1	7	3.89	1.910
ATTKS2	174	1	7	3.85	1.721
ATTKS3	174	1	7	4.25	1.894
ATTKS4	174	1	7	4.74	1.720
EOT1	174	1	2	1.82	.384
SE1	174	1	7	4.53	2.109
SE2	174	1	7	4.38	2.149
SE3	174	1	7	4.99	1.899
SE4	174	1	7	5.17	1.960
SE5	174	1	7	6.11	1.347
SE6	174	1	7	5.63	1.761
SE7	174	1	7	5.56	1.643
SE8	174	1	7	5.30	1.820
SE9	174	1	7	5.56	1.891
SE10	174	1	7	5.34	1.940
RE1	174	1	7	5.57	1.194
RE2	174	1	7	5.43	1.213
RE3	174	1	7	5.65	1.162
PS1	174	1	7	4.37	1.751
PS2	174	1	7	5.00	1.869
PS3	174	1	7	5.53	1.716
PS4	174	1	7	5.34	1.681
PS5	174	1	7	5.58	1.621
PS6	174	1	7	4.77	1.900
PS7	174	1	7	5.20	1.802
PS8	174	1	7	5.06	1.709
PS9	174	1	7	5.24	1.750
PSU1	174	1	7	3.95	1.689
PSU2	174	1	7	3.53	1.477
PSU3	174	1	7	3.45	1.571
PSU4	174	1	7	3.56	1.636
PSU5	174	1	7	3.42	1.718
AM1	174	1	7	4.59	1.720
AM2	174	1	7	4.84	1.623
AM3	174	1	7	4.73	1.659
AM4	174	1	7	4.49	1.619
AM5	174	1	7	4.39	1.772
AM6	174	1	7	4.66	1.692
TAB1	174	1	7	3.74	1.985
TAB2	174	1	7	3.63	2.018
TAB3	174	1	7	5.44	1.823
TAB4	174	1	7	5.17	1.738
Valid N (listwise)	173				

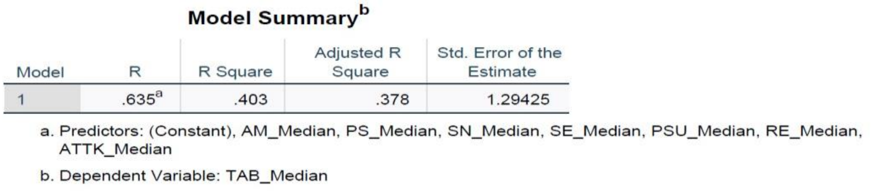

Count
0
20
40
60
80
4
37
59
74
5 years or less
6-10 years
11-15 years
over 15 years
How many years have you been using the Internet?


Count
0
20
40
60
80
100
120
52
122
Yes
No
Are you enrolled in a computing related major?


Count
100
80
60
40
20
0
97
50
13
12
1
1
18-25
26-35
36-45
46-55
56-65
over 65
Age


Count
100
80
60
40
20
0
84
90
Yes
No
Are you aware of your University's IT Security Policies?



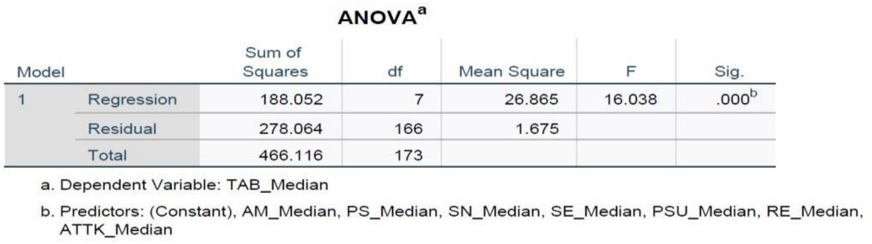


Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.635[a]	.403	.378	1.29425

a. Predictors: (Constant), AM_Median, PS_Median, SN_Median, SE_Median, PSU_Median, RE_Median, ATTK_Median

b. Dependent Variable: TAB_Median

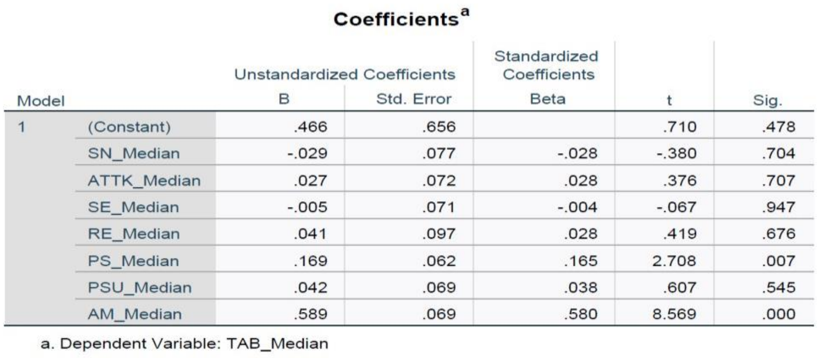


ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	188.052	7	26.865	16.038	.000[b]
	Residual	278.064	166	1.675		
	Total	466.116	173			

a. Dependent Variable: TAB_Median

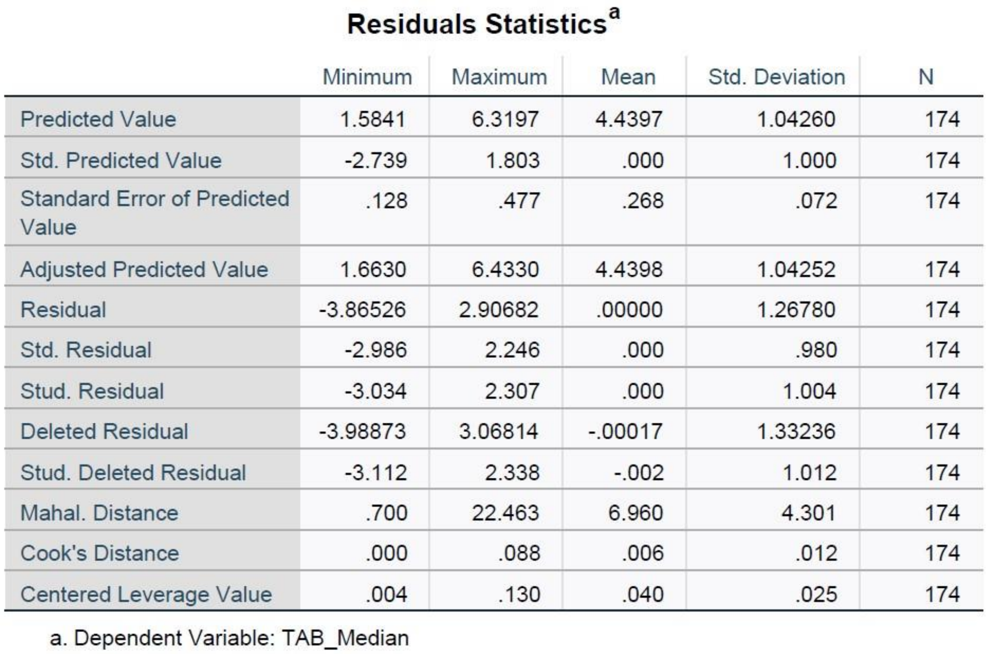
b. Predictors: (Constant), AM_Median, PS_Median, SN_Median, SE_Median, PSU_Median, RE_Median, ATTK_Median



Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	.466	.656		.710	.478
	SN_Median	-.029	.077	-.028	-.380	.704
	ATTK_Median	.027	.072	.028	.376	.707
	SE_Median	-.005	.071	-.004	-.067	.947
	RE_Median	.041	.097	.028	.419	.676
	PS_Median	.169	.062	.165	2.708	.007
	PSU_Median	.042	.069	.038	.607	.545
	AM_Median	.589	.069	.580	8.569	.000

a. Dependent Variable: TAB_Median

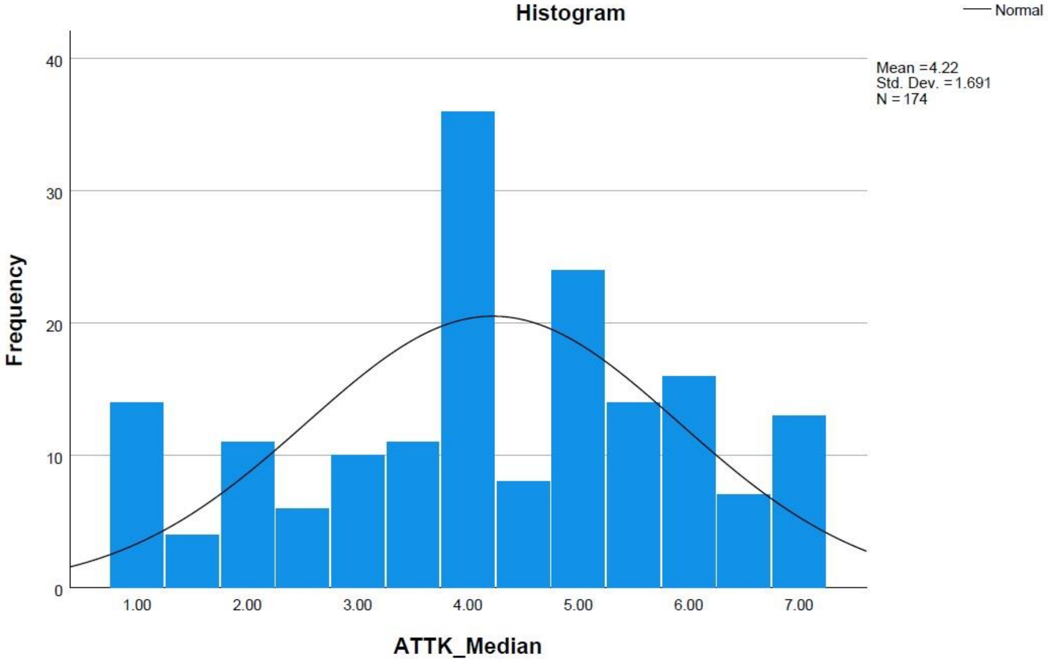


Residuals Statistics[a]

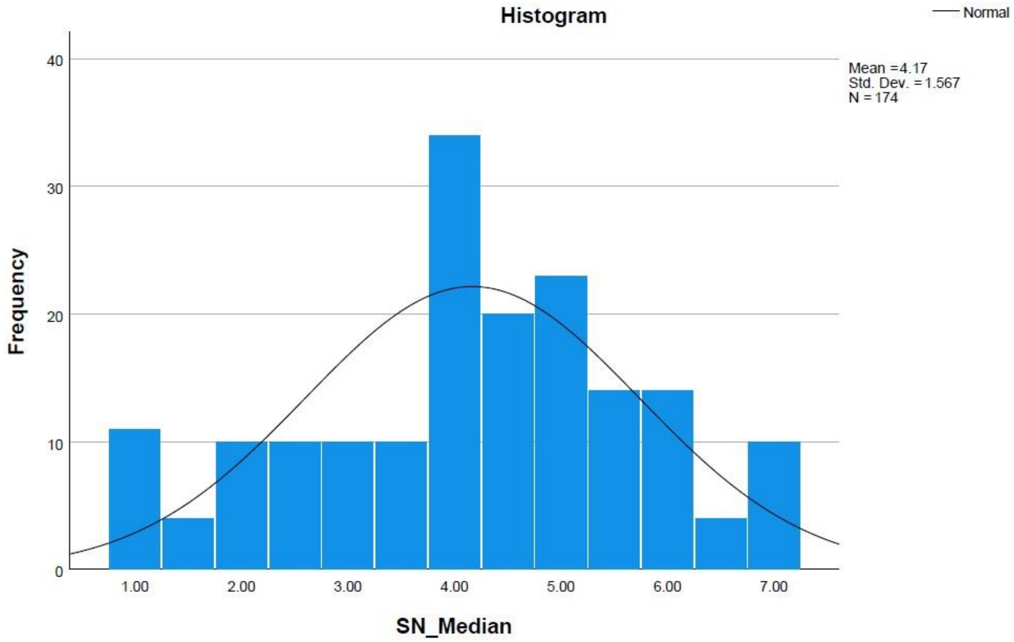
	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.5841	6.3197	4.4397	1.04260	174
Std. Predicted Value	-2.739	1.803	.000	1.000	174
Standard Error of Predicted Value	.128	.477	.268	.072	174
Adjusted Predicted Value	1.6630	6.4330	4.4398	1.04252	174
Residual	-3.86526	2.90682	.00000	1.26780	174
Std. Residual	-2.986	2.246	.000	.980	174
Stud. Residual	-3.034	2.307	.000	1.004	174
Deleted Residual	-3.98873	3.06814	-.00017	1.33236	174
Stud. Deleted Residual	-3.112	2.338	-.002	1.012	174
Mahal. Distance	.700	22.463	6.960	4.301	174
Cook's Distance	.000	.088	.006	.012	174
Centered Leverage Value	.004	.130	.040	.025	174

a. Dependent Variable: TAB_Median

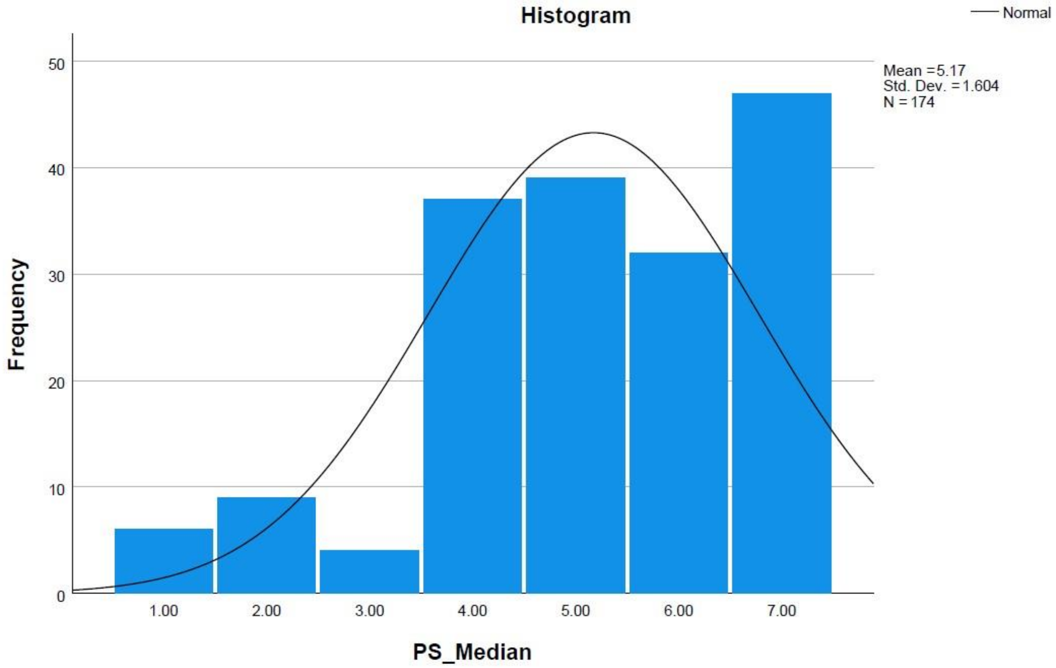
ATTK_Median



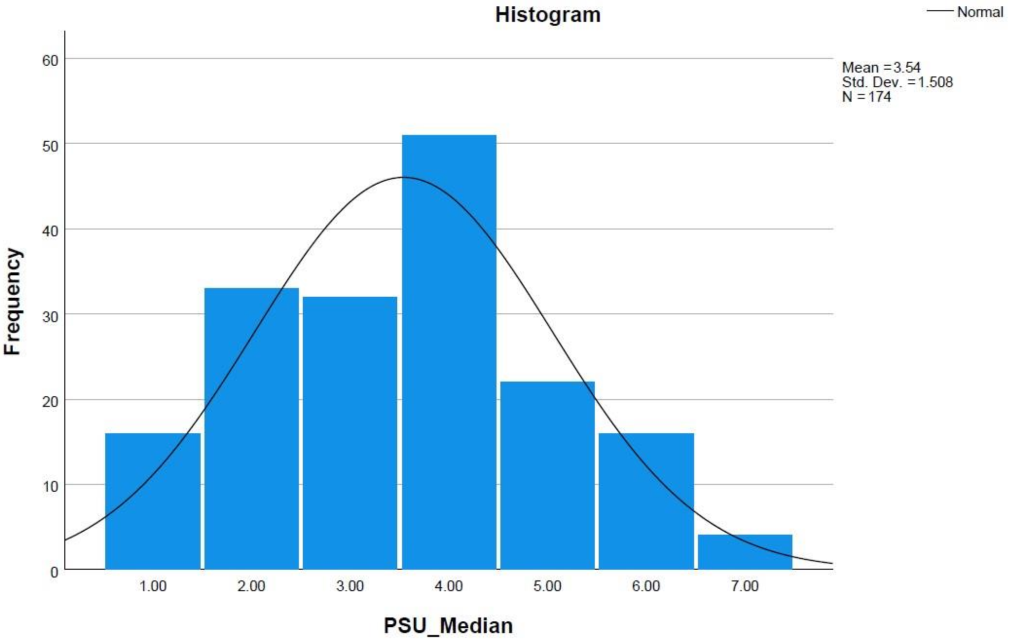
SN_Median



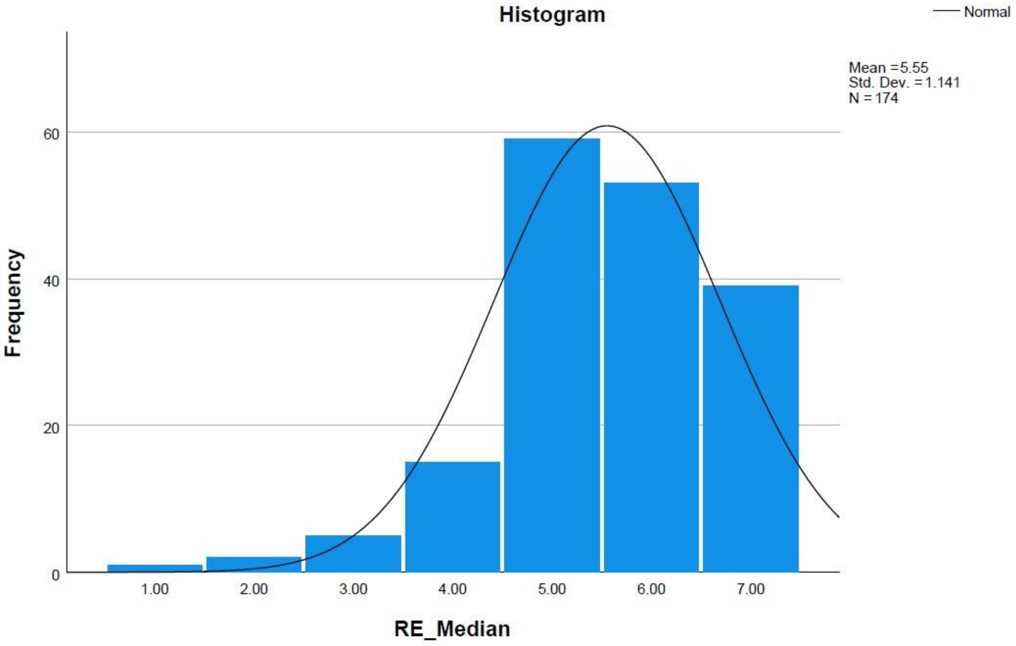
PS_Median



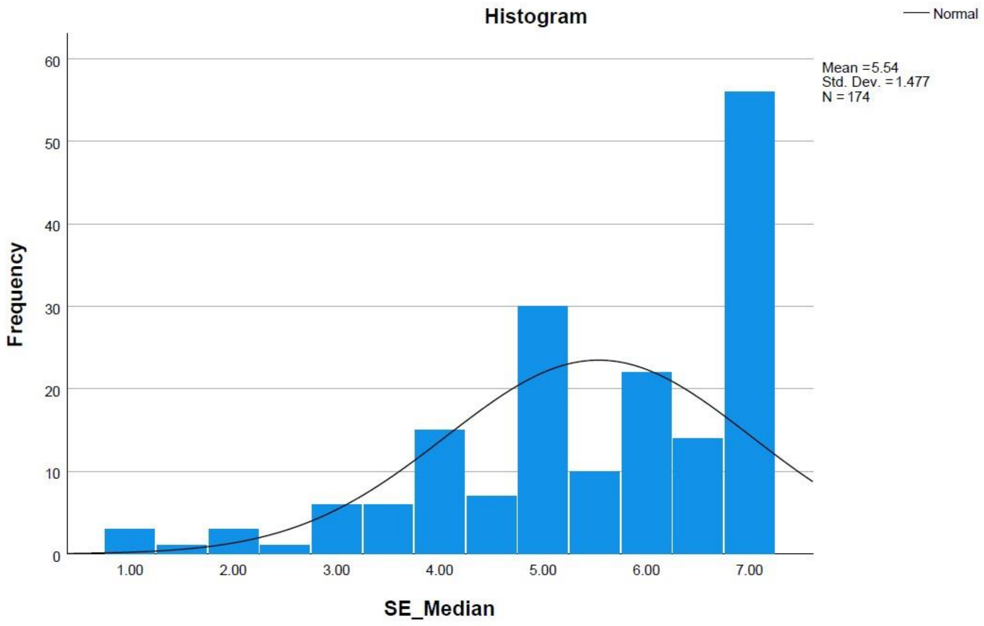
PSU_Median



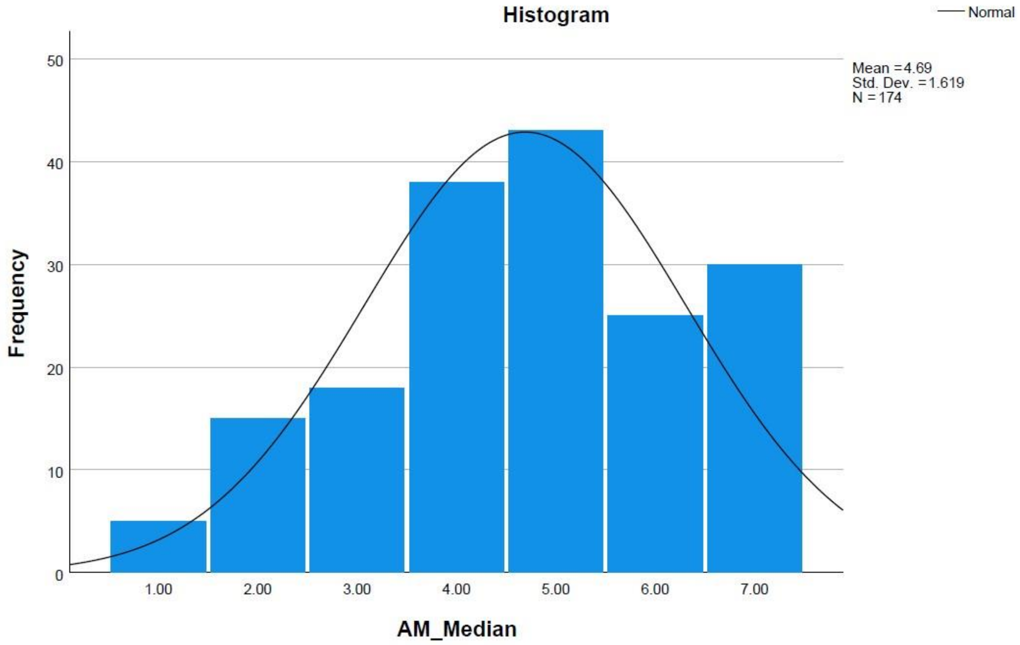
RE_Median



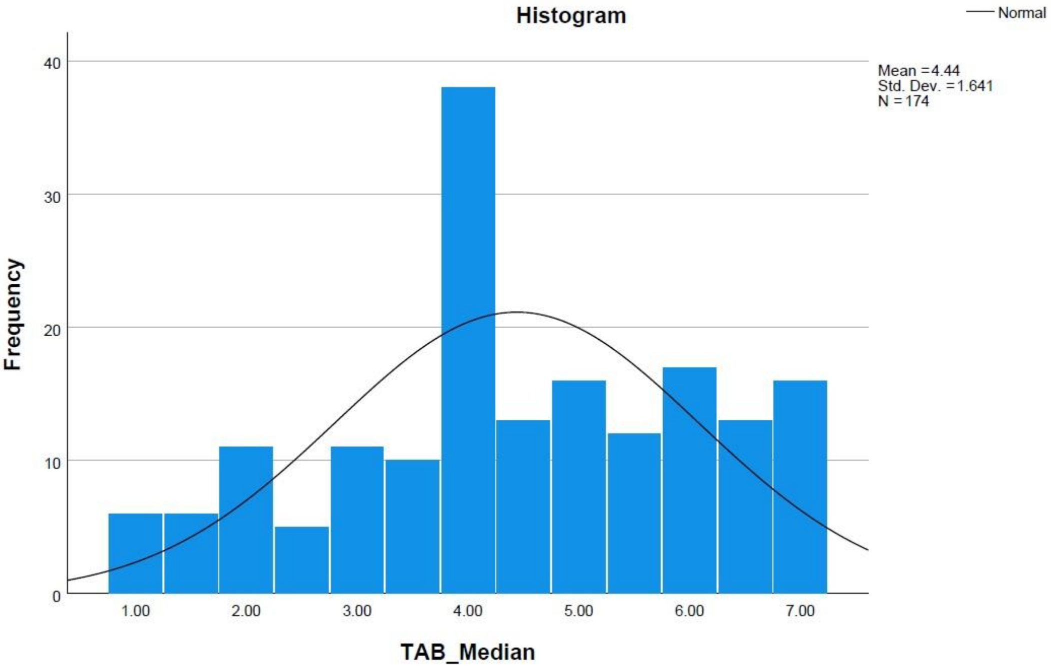
SE_Median



AM_Median



TAB_Median


Histogram
Normal
Mean = 4.44
Std. Dev. = 1.641
N = 174
Frequency
40
30
20
10
0
1.00
2.00
3.00
4.00
5.00
6.00
7.00
TAB_Median

References

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

Bock, G. W., Zmud, R. W., Kim, Y. G., & Lee, J. N. (2005). Behavioral intention formation in knowledge sharing: Examining the roles of extrinsic motivators, social-psychological factors, and organizational climate. *MIS Quarterly, 29*(1), 87-111.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of information privacy and security, 1*(3), 18-41.

Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *MIS Quarterly 40*(1), 205-222.

Chenoweth, T., Gattiker, T., & Corral, K. (2019). Adaptive and Maladaptive Coping with an It Threat. *Information Systems Management*, *36*(1), 24-39. doi:10.1080/10580530.2018.1553647

Chi, H., Yeh, H., & Hung, W.-c. (2012). The moderating effect of subjective norm on cloud computing users' perceived risk and usage intention. *International Journal of Marketing Studies, 4*(6), 95.

Chua, E. (1980). Consumer intention to deposit at banks: An empirical investigation of its relationship with attitude, normative belief and confidence. *Academic Exercise, Faculty of Business Administration, National University of Singapore*.

Cohen, J. (1992). A power primer. *Psychological Bulletin, 112*(1), 155.

Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia, 44*(1), 53-67. doi:10.1080/01611194.2019.1623343

Edwards, J. R. (1992). A cybernetic theory of stress, coping, and well-being in organizations. *Academy of Management Review, 17*(2), 238-274.

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods, 39*(2), 175-191.

Fimin, M. (2017). Are employees part of the ransomware problem? *Computer Fraud & Security, 2017*(8), 15-17.

Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research, 19*(4), 440-452.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice*, *19*(2), 139-152.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*: Sage publications.

Han, J. W., Hoe, O. J., Wing, J. S., & Brohi, S. N. (2017). *A Conceptual Security Approach with Awareness Strategy and Implementation Policy to Eliminate Ransomware*. Paper presented at the Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence, Jakarta, Indonesia. https://doi.org/10.1145/3168390.3168398

Holt, J. (1997). Current practice in software engineering: a survey. *Computing & Control Engineering Journal, 8*(4), 167-172.

Howarth, F. (2014). The role of human error in successful security attacks. *Security Intelligence Website. IBM Security Intelligence*.

Jarvenpaa, S. L., & Staples, D. S. (2000). The use of collaborative electronic media for information sharing: an exploratory study of determinants. *The Journal of Strategic Information Systems, 9*(2-3), 129-154.

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

Joshi, A., Kale, S., Chandel, S., & Pal, D. (2015). Likert scale: Explored and explained. *British Journal of Applied Science & Technology, 7*(4), 396. doi:https://doi.org/10.1016/j.jisa.2017.06.006

Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications, 35*, 128-137. doi:https://doi.org/10.1016/j.jisa.2017.06.006

Kante, M., Chepken, C., & Oboko, R. (2018). Partial Least Square Structural Equation Modelling'use in Information Systems: An Updated Guideline of Practices in Exploratory Settings. *Kabarak Journal of Research & Innovation, 6*(1), 49-67.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly, 33*(1), 71-90.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems, 11*(7), 394-413.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science, 8*(5).

Nadir, I., & Bakhshi, T. (2018). *Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques*. Paper presented at the 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan.

Ng, B.-Y., & Rahim, M. (2005). *A socio-behavioral study of home computer users' intention to practice security*. Paper presented at the 9th Pacific Asia Conference on Information Systems (PACIS 2005), Bangkok, Thailand.

O'Gorman, B. W., Candid, O'Brien, D., Cleary, G., Lau, H., Power, J.-P., Corpin, M., . . . Wallace, S. (2019). Internet Security Threat Report: Trends for 2019. *Symantec, Corp, 24*, 1-61. Retrieved from https://resource.elq.symantec.com/LP=6819?inid=symc_threat-report_istr_to_leadgen_form_LP-6819_ISTR-2019-report-main&cid=70138000001Qv0PAAS

Patyal, M., Sampalli, S., Ye, Q., & Rahman, M. (2017). Multi-layered defense architecture against ransomware. *International Journal of Business and Cyber Security, 1*(2).

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review, 13*(1), 10.

Ringle, C. M., Sarstedt, M., & Straub, D. (2012). A critical look at the use of PLS-SEM in MIS Quarterly. *MIS Quarterly 36*(1), 3-14.

Scheponik, T., Sherman, A. T., DeLatte, D., Phatak, D., Oliva, L., Thompson, J., & Herman, G. L. (2016). *How students reason about Cybersecurity concepts*. Paper presented at the 2016 IEEE Frontiers in Education Conference (FIE), Erie, PA.

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*: John Wiley & Sons.

Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N., & Diakopoulos, N. (2017). *Designing the user interface: strategies for effective human-computer interaction*: Pearson.

Singh, U. K., Joshi, C., & Gaud, N. (2016). Measurement of security dangers in university network. *International Journal of Computer Applications, 155*(1), 6-10.

Sireci, S., & Faulkner-Bond, M. (2014). Validity evidence based on test content. *Psicothema, 26*(1), 100-107.

Stanciu, V., & Tinca, A. (2016). Students' awareness on information security between own perception and reality–an empirical study. *Accounting and Management Information Systems, 15*(1), 112-130.

Sultan, H., Khalique, A., Alam, S. I., & Tanweer, S. (2018). A survey on ransomware: Evolution, growth, and impact. *International Journal of Advanced Research in Computer Science, 9*(2).

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research, 6*(2), 144-176.

Trespalacios, J. H., & Perkins, R. A. (2016). Effects of personalization and invitation email length on web-based survey response rates. *TechTrends, 60*(4), 330-335.

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management, 52*(4), 506-517.

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*, 547e559.

Venkatesh, V., Brown, S. A., Maruping, L. M., & Bala, H. (2008). Predicting different conceptualizations of system use: the competing roles of behavioral intention, facilitating conditions, and behavioral expectation. *MIS Quarterly*, 483-502.

White, J., & Simon, M. (2011). Survey/interview validation rubric for expert panel-VREP[Adobe Reader version]. Retrieved from http://dissertationrecipes.com/wp-content/uploads/2011/04/Expert-Validation-v3.pdf

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs, 59*(4), 329-349.

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior, 84*, 375-382.

Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of information systems education, 23*(4), 407-416.

Zhang-Kennedy, L., Assal, H., Rocheleau, J., Mohamed, R., Baig, K., & Chiasson, S. (2018). *The aftermath of a crypto-ransomware attack at a large academic* *institution.* Paper presented at the 27th USENIX Security Symposium (USENIX Security 18).

Zhang, X., Tsang, A., Yue, W. T., & Chau, M. (2015). The classification of hackers by knowledge exchange behaviors. *Information Systems Frontiers, 17*(6), 1239-1251.