REACTIONS TO RANSOMWARE VARIANTS AMONG INTERNET USERS: MEASURING PAYMENT EVOCATION

by

Jason Bays

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Computer & Information
Technology West Lafayette, Indiana
May 2019

THE PURDUE UNIVERSITY GRADUATE SCHOOL STATEMENT OF COMMITTEE APPROVAL

Dr. Kathryn Seigfried-Spellar, Chair

Department of Computer and Information Technology

Dr. Marcus Rogers

Department of Computer and Information Technology

Dr. Wenhai Sun

Department of Computer and Information Technology

Approved by:

Dr. Eric Matson

Head of the Graduate Program

ACKNOWLEDGMENTS

To my parents: Thank you for all of the support I've received over the years. Without your love and help during my time at Purdue, I would not have been able to make it to where I am today.

To Dr. Kathryn Seigfried-Spellar: Thank you for being my mentor and supporter during graduate school. Your guidance and experience has been incredibly valuable.

To Dr. Marcus Rogers and Dr. Wenhai Sun: Thank you for all your feedback and support during my thesis work. It is greatly appreciated!

To Sid: I have no idea how you put up with me, but I'm thankful that you do. Thank you for always being there for me and entertaining my ridiculous plans and ideas. They won't stop when we graduate, I assure you.

To Danielle: Thank you for being my research guru, friend, and go-to for impromptu plans. I look forward to many more brunches, cheese boards, and visits to DC!

To all of my friends at Purdue: Thank you for every experience we've shared together. My college experience would not have been complete without you. I look forward to many more years of fun. thank u, next!

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

SMB	Small and Medium Sized Business
STAI-6	Six-item State-Trait Anxiety Inventory (STAI-6)
STAI	State-Trait Anxiety Inventory

GLOSSARY

Amazon Mturk: an Amazon-owned website allowing for recruitment of research participants, short for Mechanical Turk (Fleischer, Mead, & Huang, 2015)

Malware: software performing actions intended by an attacker without consent of the owner when executed (Apel, Bockermann, & Meier, 2009)

Ransomware: a form of malware which encrypts files and demands payment for their return (Scaife, Carter, Traynor, & Butler, 2016)

ABSTRACT

Author: Bays, Jason C. M.S.
Institution: Purdue University
Degree Received: May 2019
Title: Reactions to Ransomware Variants Among Internet Users: Measuring Payment Evocation
Committee Chair: Dr. Kathryn Seigfried-Spellar.

Ransomware, a form of malicious software, takes users' files hostage via encryption and demands payment for their return. Since its inception, ransomware has branched into many different variants, some of which threaten users with scare tactics in order to evoke payment. For this study, four variants of ransomware were examined by presenting vignettes via an anonymous online survey. No actual malware was installed on any devices throughout this study. Their emotional responses were captured as well as their level of familiarity with information security. Responses to the survey after the simulated ransomware vignette were recorded to gauge how users would react to a ransomware attack. Data was analyzed to discover which types of ransomware evoked payment as well as if information security knowledge also had an effect on likelihood to pay. This data is intended to be used to develop better prevention methods and messaging, with an emphasis on promoting training on malware avoidance. The study found most individuals did not choose to pay, and this could be attributed to a distrust of the ransomware threat. Self-reported information security behavior appeared to decrease payment evocation, however, peer information security experience and prior exposure to malware appeared to increase payment evocation.

CHAPTER 1. INTRODUCTION

This chapter serves as an introduction to the study's research questions and problem statement. Ransomware is a serious form of malware that would pose harm to a user's system. Limitations and assumptions exist in the methodology of the current study. The limitations and assumptions are discussed.

1.1 Problem Statement

Malware, or malicious software, is one of the most common, and most damaging, attacks against a computer (Apel et al., 2009). A new and damaging type of malware, known as ransomware, takes victims' files hostage and demands payment in exchange for releasing the files (O'Gorman & McDonald, 2012). The first modern ransomware attack began in 2009, and over 16 variants have been discovered since (O'Gorman & McDonald, 2012). Ransomware employs different scare tactics in order to elicit payment. However, it is not known which type users are most susceptible, meaning more likely to evoke payment from victims, to this attack. Due to the unknown nature of response to these variants, prevention methods often focus solely on the most generic type of malware, and may not address the types users actually respond to the most.

1.2 Scope

For this research, four variants of ransomware will be studied - a normal variant, a countdown variant, a fake law enforcement variant, and an upload threat variant. The scope was defined by types of ransomware identified by security research organizations such as Symantec and MalwareBytes Labs. These organizations found these scare-tactic variants of ransomware to be the most common attacks in recent years. Other forms of ransomware do exist, but they tend to fall under similar variants to the four used in the study (O'Gorman & McDonald, 2012). The population for this study will be adults aged 18 or older within the United States. Any individual owning a personal computer device is vulnerable to malware.

Android or other mobile based ransomware is beyond the scope of this study, but the methods of prevention from a human-behavioral standpoint would be similar for mobile devices.

1.3 Significance

Malware is a multi-billion dollar industry for cybercriminals (Morgan, 2016). Studies have shown technical and software intervention of ransomware attacks is only a part of the solution. The human-behavioral aspect of an attack is just as important to prevention because users may circumvent technical solutions or mistakenly download infected software. Training is a vital component of malware prevention, as users need to understand the threats they may be subjected to. Understanding why victims choose to respond or pay the ransom will assist the security community in developing effective messaging and training for ransomware prevention. If ransomware authors are unable to effectively elicit payment, they lose their motivation for creating and initiating these attacks.

Ransomware affects both individuals and businesses, with 49% of small-to-medium sized businesses reporting it to be one of the most serious threats they face (Lab, 2016). Businesses may lose patient records, financial documents, backups, and other documents vital to the operation of the organization. Individuals may lose photos, videos, personal documents, andother personal data. Modern ransomware also has the ability to spread to backups in many cases (Kharraz, Robertson, Balzarotti, Bilge, & Kirda, 2015). This indicates prevention is an important step, because simply restoring from a backup after the fact may not be possible. In addition, ransomware has become more lucrative over time because of how many individuals are forced to pay the ransom. The average ransom demand has increased from $300 in 2015 to over $1000 in 2017 (Korolov, 2017). Ransomware is an overarching threat to both individuals and businesses, and there needs to be a greater understanding of how it affects these sectors.

1.4 Research Questions

The current study includes the following research questions:

1. What variant of ransomware is most likely to evoke payment from users?

The study also includes the following ancillary question:

Does familiarity with secure computer and internet behaviors impact payment response in participants?

1.5 Manipulation Check

The current study includes the following manipulation check:

- Are participants in a heightened state of anxiety after undergoing a mood induction activity?

1.6 Assumptions

The assumptions for this study include:

- A participant's emotional state is moderate enough when beginning the survey in order to induce mood.
- A participant will be actively engaged throughout the survey and study.
- The participant is using a device containing at least some data they consider valuable.

1.7 Limitations

The limitations for this study include:

- Because installing true ransomware on a user's system is unethical and dangerous, the ransom screens were simulated using software. True reactions to actual ransomware infections cannot be collected.
- Only the initial response can be studied, not the final decision whether or not to pay.

- The simulation will not take into account technical prevention methods the user has on their system, such as antivirus software.

1.8 Delimitations

The delimitations for this study include:

- As participants will realize the infection is a simulation, anxiety was instead produced artificially.
- Only desktop ransomware was tested; ransomware which runs on Android and other mobile devices was out of scope.
- Only four variants of ransomware are studied in this research.

1.9 Summary

This chapter provided the scope, significance, research question, assumptions, limitations, delimitations, definitions, and other background information for the assessment of human-behavioral responses to malware. The main purpose of this study is to determine whether or not the variant of ransomware and knowledge of information security has an effect on participants' willingness to pay a ransom. This study is focused on ransomware from a

human-behavioral perspective, intended to assist in developing prevention methods and training. This study will consist of a survey with four different ransomware vignettes assigned to participants in the United States, and this survey will measure likelihood of each vignette to evoke payment from participants.

The next chapter will outline relevant literature. A background to computer crime and malware will be provided. Relevant literature specific to malware, information security behavior, and security behavior will be analyzed.

CHAPTER 2. REVIEW OF RELEVANT LITERATURE

This chapter provides an overview of the body of literature relevant to ransomware. Specifically, literature was reviewed for human-behavioral prevention and awareness methods. An overview of ransomware and its function are provided, followed by an explanation of information security culture and relevant prevention methods. Relevant statistics are provided to show the impact of ransomware.

2.1 Introduction to Cybercrime

While modern technology has brought many innovations and improved society as a whole, criminals have also adapted to using the computer as a tool for crime. Cybercrime involves the abusive use of a computer in one of three manners: as a tool, as a target, or as an incidental in a crime (Bossler, Holt, & Seigfried-Spellar, 2017). In many cases, traditional crimes such as fraud, identity theft, and stalking have taken on new forms on the internet. For example, stalking now exists via social media sites and sites which post individuals' addresses and personal information. Some crimes, such as hacking and network intrusion, exist solely in the digital realm. It has been estimated cybercrime will cost the global economy $6 trillion annually by 2021. (Morgan, 2016). In addition, McAfee has warned that cybercrime may have a lasting effect on the U.S. economy due to its effects on U.S. businesses (Hyman, 2013). Because of this, it is vital for law enforcement and researchers to understand cybercrime and who commits it. Preventing the public from falling victim to these types of attacks benefits the public as a whole. This study will examine ransomware, a form of malware, which can be described as a form of extortion. Using messaging which promotes fear, and taking victims' information hostage, ransomware is a very modern threat which extorts over $200 million from victims each year (Corrigan, 2017).

2.2 Malware

One of the most common threats in a computer information system is malware. A shortened form of "malicious software", malware can take the form of any piece of code designed to harm a system or its users. Apel et al. (2009) defined malware as, "software performing actions intended by an attacker without consent of the owner when executed" (p. 891). Examples of malware, which has been a major threat to computing system since around 1990, include worms, trojan horses, and viruses (Zolkipli & Jantan, 2010).

Viruses attempt to execute harmful code on a user's system and requires host action, whereas a worm also uses the user's internet connectivity or email to replicate itself on other systems. Trojan horses act as benign or useful software, but they contain harmful code which runs in the background. Malware first was identified on PCs around 1986 (Milošević, 2013). Early viruses focused on damaging files or simply annoying the victim. In the mid-1990s, viruses began to grow more complex with the large userbase of Microsoft Windows (Milošević, 2013). Worms were rampant in the early 2000s, attaching themselves to mail clients and mailing themselves to the user's entire address book. Whereas early malware was mainly used to simply damage files, modern malware is primarily used to make money for the malware author. Modern malware may attempt to steal users' personal information, insert advertisements into web browsers or other programs, or demand payment (Apel et al., 2009). This study will focus on a modern form of malware, known as ransomware.

2.3 Ransomware

Ransomware is a form of malware which infects the host computer, encrypting the files on that computer's storage, and demanding a payment for the decryption of the user's files. The earliest form of cyber-extortion, predating modern ransomware, was identified in 1989, known as the "PC CYBORG" or "AIDS" Trojan (Hampton & Baig, 2015). This trojan spread via an infected floppy disk. It placed an infected file onto the host machine, lay dormant for a period of time to evade suspicious, and finally encrypt files under the guise of the user breaking a license agreement. This software would demand $189 from the user, which had to be mailed to Panama in order for a decryption disk to be mailed. Despite these early attacks, ransomware would not become common until the early 2000's when the internet could be used to spread this type of attack (Hampton & Baig, 2015).

According to Symantec, one of the United States' largest cybersecurity firms, modern Ransomware was first seen around 2009 in Russia (O'Gorman & McDonald, 2012). This type of ransomware, still the most common, locks the user’s screen and demands payment before the computer can be used. Modern ransomware packages can encrypt the user’s entire file system in about 15 minutes. These modern ransomware packages connect to the attacker’s servers in order to provide the decryption key upon payment, if the decryption is even possible. Ransomware authors are able to evade detection through the use of anonymous payment such as Bitcoin wallets (Salazar, 2015). Bitcoin is a decentralized cryptocurrency established in 2009 which provides for anonymous and verified transactions (Barber, Boyen, Shi, & Uzun, 2012). According to Kharraz et. al. (2015), “Bitcoin keys are not explicitly tied to real users, although all transactions are public. Consequently, ransomware owners can protect their anonymity and avoid revealing any information that might be used for tracing them” (p. 14). Some of the most infamous ransomware attacks, such as Cryptolocker and WannaCry, have used this method to collect their payment.

However, the most common method in 88.2% of ransomware samples studied by Kharraz et. al. (2015) was the use of prepaid online payments, such as Moneypak or Ukash cards. These services provide anonymous transfer of money and are not tied to a banking institution. Some ransomware attackers sell the vouchers they receive online through forums or chatrooms to make the money even harder to trace (Salazar, 2015).

2.3.1 Technical Details

It is also important to understand how ransomware operates from a technical standpoint, as ransomware can be a complex form of malware, and the methods for developing technical prevention methods is different than other forms. While researchers can sometimes develop solutions to remove ransomware, other forms cannot be removed without data loss. Scaife et al. (2016) identified three main behavior patterns of ransomware. The first, which they deemed Class A, operates by opening each file on the system, reading the file, writing the encryption in-place, and then closing the file. This type also may rename the file to further obfuscate the user’s information. The second type, Class B, functions much like the first, except it moves each file out of its current directory, encrypts the data, and then moves it back. If the malware does provide for decryption, it keeps a log of each file and where it was moved. The final type, Class C, operates by opening the initial file, creating a new file, copying the encrypted contents to the new file, and deleting the initial file.

Kharraz et al. (2015) further analyzed the activity which characterizes a ransomware attack. Recent attacks encrypt files using an AES-256 encryption key, and this key is encrypted using a 1024-bit RSA public key. These encryption methods are cryptographically strong, and cannot easily be brute forced or decrypted without the key. These keys are generated and stored on the attacker's command server. Older ransomware attacks would generate and store the key locally, but this allowed victims to extract the key from memory. WannaCry, one of the most infamous ransomware attacks, would store its key, user ID, total encrypted file count, and total file size to a registry entry it created upon infection (Chen & Bridges, 2017). Newer ransomware samples were also found to employ file system functions which search for network drives, and the ransomware will attempt to encrypt those as well (Kharraz et al., 2015). Hampton and Baig (2015) noted most attacks build on the success of the previous and implement new, more technically secure methodology. Most ransomware samples were found to avoid encrypting system files, but some attacks, such as the Seftad attack, encrypt the bootloader and demand a ransom before the system is allowed to boot. The bootloader is located on the first sector of a system's hard drive, and is necessary for a computer to load the operating system. Encrypting it prevents the computer from being able to complete the boot process.

The next major step in an attack is locking the computer, which is characteristic of modern ransomware (O'Gorman & McDonald, 2012). The malware will create a new desktop on the victim's system, or in some cases, download a Hypertext Markup Language (HTML) page and load it into the victim's Internet Explorer browser (Kharraz et al., 2015). The victim's system will then display the downloaded desktop or web page, which demands a ransom and will lock the system until it is provided. Keyboard shortcuts, and other methods of switching active windows on the desktop, will be disabled.

The final step in an attack is payment and decryption, if the user decides to proceed with a payment. Online payment methods are the most common form of payment, using services suchas Moneypak and Ukash. Bitcoin is also a common form of ransom. The ransomware will connect to its control server, verify the payment, and at this point may decrypt the data using the previously generated keys. There is no guarantee a payment will successfully decrypt the files, especially if the victim modified their system in response to the infection. Because ransomware is a criminal activity, there is a possibility the decryption offer is a scam. However, many ransom messages mention their legitimacy and willingness to decrypt successfully because of the attacker's desire to entice other victims to pay the ransom. The methods discussed in this section primarily address malware written for Microsoft Windows systems. Ransomware written for Mac OS and Android are beyond the scope of this study, but as this study primarily focuses on the human-behavioral response and messaging of the attack, there should not be many differences.

2.3.2 Impact

The impact of ransomware comes from two main sources - the financial impact of paying the ransom or the financial impact of not paying the ransom and subsequently losing any files which are not backed up and possibly having personally identifiable information released. Businesses, in particular, must face this choice if they have data integral to the operation of the company locked by the ransomware Mansfield-Devine (2016). Home users may also not have sufficient backups and choose to pay the ransom.

Calculating the amount of ransoms paid is difficult due to the anonymous nature of the payments and payment sources. Liao, Zhao, Doupé, and Ahn (2016) analyzed online sources to identify 968 Bitcoin wallet addresses belonging to the CryptoLocker ransomware. Analyzing the transactions sent to these addresses resulted in 1,128.40 Bitcoin being paid. Because of the extreme fluctuations in Bitcoin value, this could range anywhere between $310,000 and $1.1 million in damages (Liao et al., 2016). It is also important to note CryptoLocker also accepted MoneyPak payment, which is what the majority of payments from the United States were made in. MoneyPak is a prepaid payment method and not tied to any banking institution. As there was no discernable benefit to the user for using either payment method, it is likely a large amount of payments were also made in MoneyPak, which cannot be traced. Overall, the FBI estimates a total $27 million was paid in ransom to the developers of Cryptolocker when all payment methods are taken into account (Richardson &

North, 2017). According to Brewer (2016), the FBI estimated there would be over $1 billion in damage done from ransomware in 2016. In the second quarter of 2015, security researchers identified over four million ransomware samples on infected hosts.

The business impact of attacks is also hard to measure, but of particular interest is the healthcare industry. Attackers typically combine phishing campaigns in order to launch a ransomware attack against entities such as hospitals (Mansfield-Devine, 2016). The healthcare industry commonly stores important patient records which would be a devastating loss to the business if completely erased. In addition, healthcare organizations often run on specialized or legacy hardware which is susceptible to attack. In August 2016, security firm FireEye saw the Locky ransomware being dropped in Word files to healthcare organizations in the United States, Japan, Korea, and Thailand (Mansfield-Devine, 2016). In addition, Intel Security reported 24 ransomware attacks aimed at hospitals and other healthcare facilities in the first six months of 2016 (Mansfield-Devine, 2016).

The other major group vulnerable to attack is the small business market. Kaspersky, an antivirus and cybersecurity firm, found 49% of small to medium sized businesses (SMB) consider cryptomalware to be one of the most severe attacks they worry about in their organization (Lab, 2016). This indicates small businesses have a vested interest in developing effective prevention methods and understanding why their employees may fall victim to this type of attack. Small businesses are often targeted because they don’t have large enterprise backups and often lack sophisticated data handling policies.

2.3.3 Economics of Ransomware Market

Some work has been done in analyzing the economic drive behind ransomware attacks. Bayoumy (2018) wrote a study regarding the economic market of ransomware-as-a-service. Vendors on black market sites offer prebuilt ransomware for sale, allowing those without the technical knowledge to write their own ransomware to perform ransomware attacks. The authors found many ransomware packages being sold on black markets are fake or nonfunctional, indicating some individuals are making money by scamming would-be ransomware attackers.

For those considered legitimate sales of customizable ransomware, Bayoumy (2018) found ransomware authors engage in profit partnership plans with those they sell the ransomware package to. For example, the Ginx ransomware was offered at $1500, with the purchaser keeping 70% of the profit. This decreases to $500 in which the purchaser keeps 50% of the profit. However, it does not appear a large amount of people purchased this variant, and the authors found the overall amount of people purchasing ransomware packages is low, partly in fact due to the high amount of scams on the market.

Caulfield, Ioannidis, and Pym (n.d.) created a model for determining how ransomware demand amounts are set. Their model takes into account companies and their willingness to pay, ransomware authors and their desire to maximize revenue, price perturbation, information sharing, and reliability. This study found the ability of ransomware to generate profit does not decrease significantly until 70% of individuals in the population backup their computer. Their model also demonstrated how ransomware authors are able to alter the price of their ransomware to gauge willingness to pay in the population, and that learning this vulnerability of their target population can lead to more revenue over time.

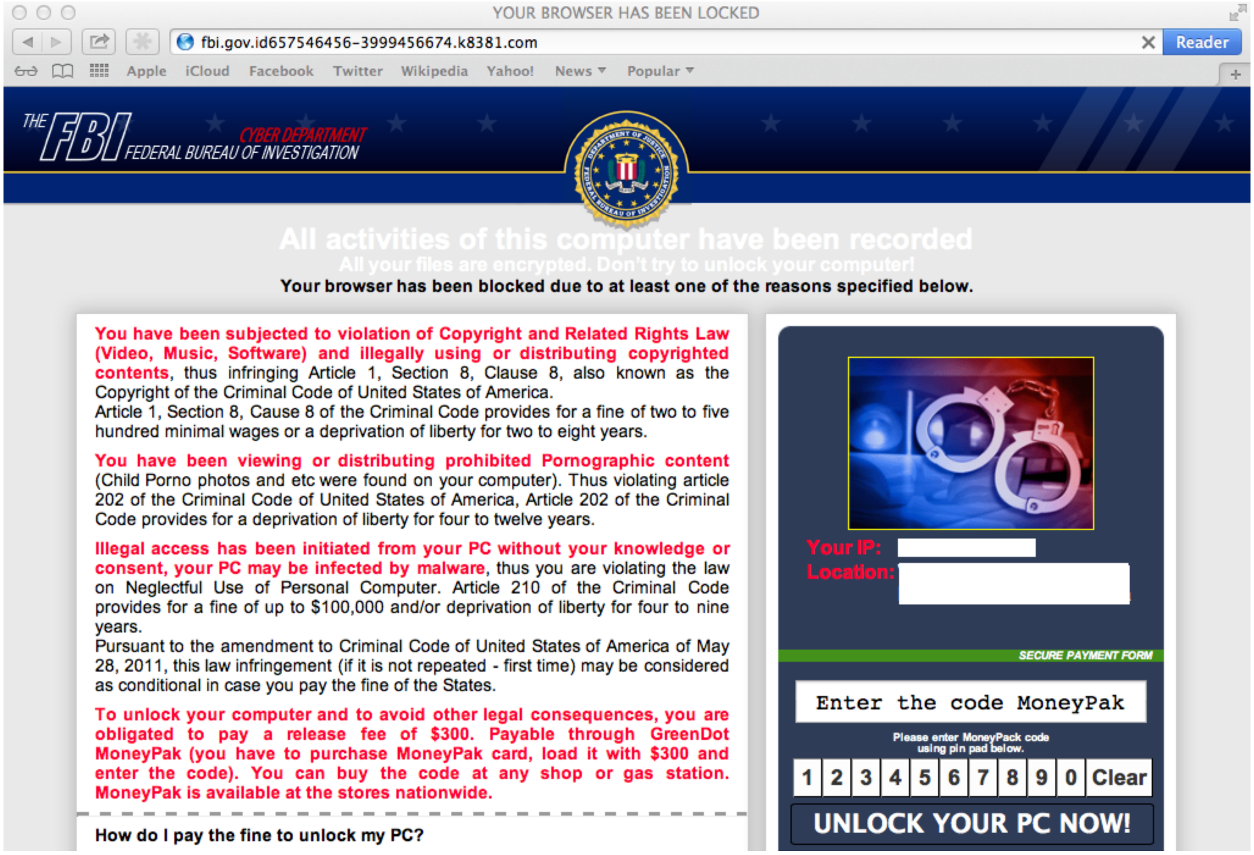
Hernandez-Castro, Cartwright, and Stepanova (2017) also investigated an economic model of ransomware, taking into account actual information from previous cases of ransomware. The authors also found information gathering from attackers can go into ransom pricing in complex variants. They cited the Shade ransomware, which could install a remote access exploit onto a computer and discover the victim’s financial information, attempting to determine how much they could afford to pay.

It was also found some ransomware authors are open to bargaining (Hernandez-Castro et al., 2017). The Jigsaw ransomware attack, for example, demanded $150 by default, but the authors accepted up to a 17% discount. CryptoMix was found to have accepted up to a 67% discount.

This literature shows ransomware contributes to a unique economy often paralleling business economics. Ransom authors use bargaining and data available within the malware realm to set their prices and sometimes allow for negotiation. This shows the importance of the ransomware price, and shows ransomware authors are actively monitoring payments to discover what price point people will respond to the most.

2.4 Variants of Ransomware

One of the more unique elements of ransomware compared to other malware types is its use of scare tactics to elicit payments. Basic ransomware packages simply lock the system and demand payment, but other variants use imagery and wording which attempt to scare the user into paying. Symantec, as early as 2012, identified 16 variants of ransomware (O'Gorman & McDonald, 2012). One of the more common variants is ransomware employing a fake message from law enforcement. This form typically informs the user their computer has been used for serious crimes such as distribution of child pornography or terrorism, and the user must pay within a certain time to avoid being placed under arrest. This is usually combined with seals or other imagery of the associated law enforcement agency. An example of this is the 2016 FBI Ransomware attack, as shown in Figure 2.1.


YOUR BROWSER HAS BEEN LOCKED
fbi.gov.id657546456-3999456674.k8381.com
Reader
Apple
iCloud
Facebook
Twitter
Wikipedia
Yahoo!
News
Popular
THE FBI
CYBER DEPARTMENT
FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

All activities of this computer have been recorded

All your files are encrypted. Don't try to unlock your computer!

Your browser has been blocked due to at least one of the reasons specified below.

You have been subjected to violation of Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted contents, thus infringing Article 1, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.
Article 1, Section 8, Cause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno photos and etc were found on your computer). Thus violating article 202 of the Criminal Code of United States of America, Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law on Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to $100,000 and/or deprivation of liberty for four to nine years.
Pursuant to the amendment to Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated - first time) may be considered as conditional in case you pay the fine of the States.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $300. Payable through GreenDot MoneyPak (you have to purchase MoneyPak card, load it with $300 and enter the code). You can buy the code at any shop or gas station. MoneyPak is available at the stores nationwide.

How do I pay the fine to unlock my PC?

Your IP: [redacted]
Location: [redacted]

SECURE PAYMENT FORM

Enter the code MoneyPak

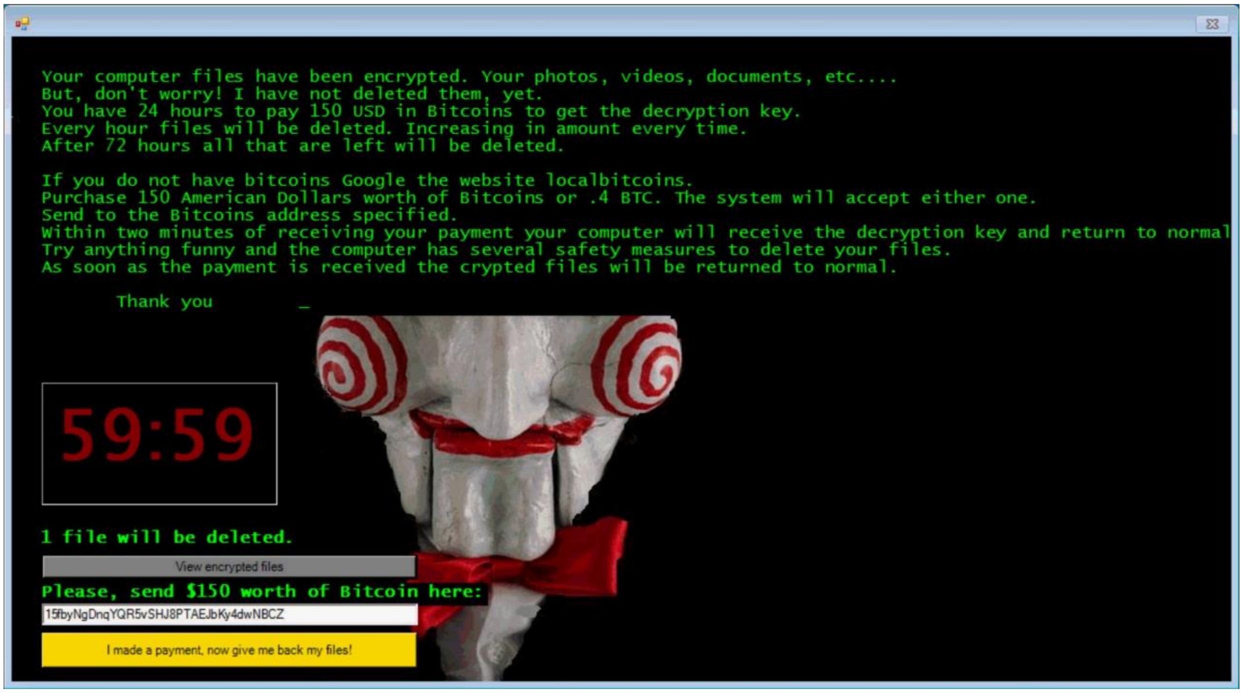
Please enter MoneyPack code
using pin pad below.

1 2 3 4 5 6 7 8 9 0 Clear

UNLOCK YOUR PC NOW!

Figure 2.1. Example FBI Ransomware from Segura (2016)

A second variant of the typical ransomware package is one which uses time as the primary tactic. This variant will display a countdown clock, often only giving the user a few hours to pay. A recent example of this tactic is the Jigsaw ransomware (Constantin, 2016), as shown in Figure 2.2. This variant sometimes also deletes files in phases, starting with a few files every hour, to thousands after a day. The Jigsaw ransomware also threatens to delete files if the user attempts to delay the countdown by restarting the system.



```
Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.

If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return to normal
Try anything funny and the computer has several safety measures to delete your files.
As soon as the payment is received the crypted files will be returned to normal.

       Thank you        _
```

59:59

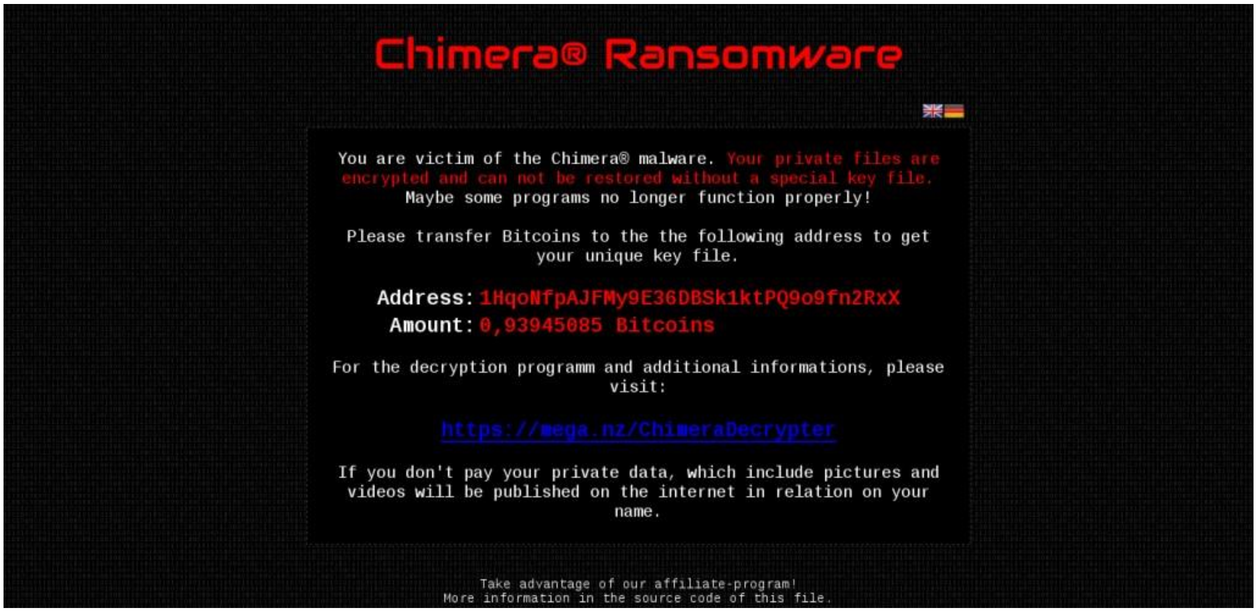
1 file will be deleted.

Please, send $150 worth of Bitcoin here:

15fbyNgDnqYQR5vSHJ8PTAEJbKy4dwNBCZ

Figure 2.2. Example countdown variant from Constantin (2016)

A third variant of ransomware, identified by antivirus manufacturer Malwarebytes, goes beyond simply threatening the loss of files, but also threatens to publish the victim's files to the internet (Malwarebytes, 2016). This attempts to scare the user into payment by instilling the belief their personal pictures and documents will be uploaded for the public to see. While this variant does not usually follow through with the upload, victims could still be manipulated into paying simply by making the threat. An example of this, the Chimera Ransomware attack, is shown in Figure 2.3.



Chimera® Ransomware

You are victim of the Chimera® malware. Your private files are encrypted and can not be restored without a special key file.
Maybe some programs no longer function properly!

Please transfer Bitcoins to the the following address to get your unique key file.

Address: 1HqoNfpAJFMy9E36DBSk1ktPQ9o9fn2RxX
Amount: 0,93945085 Bitcoins

For the decryption programm and additional informations, please visit:

https://mega.nz/ChimeraDecrypter

If you don't pay your private data, which include pictures and videos will be published on the internet in relation on your name.

Take advantage of our affiliate-program!
More information in the source code of this file.

Figure 2.3. Example document upload threat from Malwarebytes (2016)

While there are many different ransomware packages, these four types of ransomware (normal threat, countdown, law enforcement, and extortion) are where the majority of attacks fall into, according to the literature. These variants will be the ones utilized in this study.

2.5 Information Security Culture

There exists the belief today businesses should implement holistic policies, training, and awareness campaigns which provide for an overarching information security culture. Since many ransomware attacks are the result of phishing campaigns and social engineering of the victim, effective training and awareness could be expected to decrease the number of attacks. According to Martins and Elofe (2002), “By instilling an information security culture, information security practices such as a clear desk policy and controls such as encryption will be accepted as the way in which things are done. These practices will aid in solving the threat of internal security breaches and prevent external security breaches” (p. 205).

Implementing effective prevention policies and training is of interest to business users, but home users also benefit from general awareness. Law enforcement, community organizations, and antivirus manufacturers should encourage awareness among home users. Implementing solely technology-based prevention methods is not effective (Bulgurcu, Cavusoglu, & Benbasat, 2010). Bulgurcu et al. (2010) found in their study of information security policies employees are influenced by their attitude, normative beliefs, and self-efficacy when following the information security policy. If an employee does not care about the policy or understand the importance of following it, they will be less likely to follow it.

2.6 Prevention Methods

Many technical solutions exist for ransomware prevention, such as network scanning and antivirus policy enforcement. This study, however, primarily views ransomware prevention from a human perspective. A body of literature exists suggesting awareness and education is important to preventing attacks against information security. Luo and Liao (2007) writes on the importance of awareness in preventing ransomware attacks, "Companies should take steps to raise employee awareness, from altering employees about new threats and existing policies and procedures, to brown bag luncheons and asking employees to sign documents attesting to their security and confidentiality standards" (p. 201). Since ransomware is a relatively new type of attack, this study aims to fill the gap in understanding which types of ransomware users are most likely to fall for, as well as what role information security awareness plays in their reaction.

White (2015) showed in their study education and understanding of threats plays the greatest role in reducing threats, finding that implementation of technology alone did not reduce security incidents. Security is often an issue of people more than technology. The National Institution of Health (NIH), in coordination with resources from the United States Office for Civil Rights, Federal Bureau of Investigation, and Federal Trade Commission, published a list of ransomware prevention steps (Pope, 2016). These steps include understanding the scope of ransomware attacks, ensuring all employees receive proper ransomware training, backing up important files, encrypting private data, implementing technical safeguards, and staying informed. In regards to ransomware training, the NIH recommends training staff on both detecting an active infection as well as preventative steps. Sittig and Singh (2016) published a socio-technical approach to ransomware prevention, noting users must be aware not to follow unsolicited web links, how to avoid falling for scams, and knowing how to react and where to report the attempt. All of these actions contribute to an information security culture which encourages prevention and mitigation of attacks.

2.6.1 Information Security Behavior

Studies have been conducted regarding information security behavior among the general population. Aytes and Conolly (2003) studied gender differences in cybersecurity risk behaviors, finding women are more worried about engaging in risky behavior, while men were more willing to take risks. Men, however, self-reported higher levels of adherence to cybersecurity behavior than women. As previously discussed, Bulgurcu et al. (2010) found attitude, normative beliefs, and self-efficacy contribute to compliance to information security behavior and policy. This indicates those who put the responsibility on themselves to protect their job and security may adhere better to information security policy.

A study by Anderson and Agarwal (2010) aimed to investigate what effect messaging had on compliance with security policy. A loss aversion approach, which included negative messaging and threatening of consequence for non-compliance, was found to be less effective than positive messaging describing the positive effects adherence will have. This shows messaging can drive behavior, indicating the messaging of ransomware itself within this study may have an effect on user behavior. The study by Anderson and Agarwal (2010) states, “From the perspective of persuasive messaging, although others have alluded to and tested the effects of framing and self view on attitudes and intentions...prior research has not examined how these variables interact to influence norms” (p. 638). Examining the variants of ransomware and their associated messaging may reveal different responses and different behavior among groups, especially those less familiar with information security culture.

2.7 Summary

This chapter provided a review of the relevant literature in ransomware research. An introduction to malware and computer crime was provided, and the concept of ransomware was explored. Ransomware is a form of malware which encrypts a host system's files and demands a payment for the decryption of the user's files. This was related to information security behavior and information security culture. Information security culture promotes awareness and training of common attacks and how to avoid them. A gap, how users react to different variants of ransomware, was identified in the research which will be explored by this study. The next chapter will provide an overview of the methodology of the study.

CHAPTER 3. FRAMEWORK AND METHODOLOGY

This section provides an overview of the methodology used in the study of responses to ransomware. Participants were recruited online to take an online survey and activity, and after completing a difficult puzzle, took a survey in which a ransomware attack was simulated. This survey then asked about the response to the ransomware attack and gauge emotional response, the likelihood of the participant to pay the ransom, and their knowledge of information security as a whole. This data was analyzed to determine which factors and which ransomware variants contribute to response and likelihood of payment.

3.1 Hypotheses

Although research has been conducted on malware as an overarching issue, research has not addressed ransomware from a human-behavioral standpoint, meaning it is not yet understood why individuals respond to certain forms of ransomware over others. This study analyzed which variants of ransomware was most likely evoke payment from an individual, as the different forms have evolved to include scare tactics and other psychological methods. Based on the literature (O'Gorman & McDonald, 2012), and the use of methods described by researchers such as Constantin (2016), the following hypotheses were developed:

H_1: Individuals will report a higher likelihood to pay when exposed to ransomware with scare tactics.

In addition, the following ancillary hypothesis was also developed:

H_A: Familiarity with secure computer and internet behaviors will decrease likelihood to pay the ransom in participants.

3.2 Survey Design

This anonymous study took place online. Participants were asked to complete the study on their personal computer. The survey was conducted on personal devices to increase the perceived severity of the simulated ransomware attack. Participants were randomly assigned to either the experimental group or the control group. The experimental group went through a mood induction activity, which was designed to induce anxiety. The control group did not experience mood induction. Once this activity was complete, participants completed an online survey. The online survey consisted of the mood induction activity for those in the experimental group, an anxiety inventory, a malware vignette, and a final set of questions related to information security behavior. A summary of this survey methodology can be found in 3.1.

Participants in the experimental group were instructed they must complete a puzzle activity in order for the study to continue. A sudoku puzzle was presented to these participants. This puzzle was difficult and did not provide positive feedback, a method considered effective by the literature to increase negative mood (Westermann, Spies, Stahl, & Hesse, 1996). Immediately following the anxiety induction, the participants were instructed to begin the survey. Research has shown the importance of beginning the study immediately following mood induction in order to produce the most realistic results (Isen & Gorgoglione, 1983).

Following the mood induction, the survey and simulation began. There was an initial set of questions asking about the participant's mood. Since this study desired participants to be in an anxious mood, anxiety was measured using the Six-item State-Trait Anxiety Inventory (STAI-6). The State-Trait Anxiety Inventory (STAI) is a very common scale, measuring anxiety in participants (Marteau & Bekker, 1992). This scale has been regarded as both reliable and valid. However, the STAI is long, consisting of 40 scale items. Marteau and Bekker (1992) developed a shorter six-item version of this scale, which retains the reliability and validity, and the shorter length helps maximize response rates and shortens the amount of time participants have to spend answering a given scale. This is a likert-type scale, designed to assess whether participants are currently feeling anxious. This was used in the manipulation check to see whether or not the mood induction had an effect.

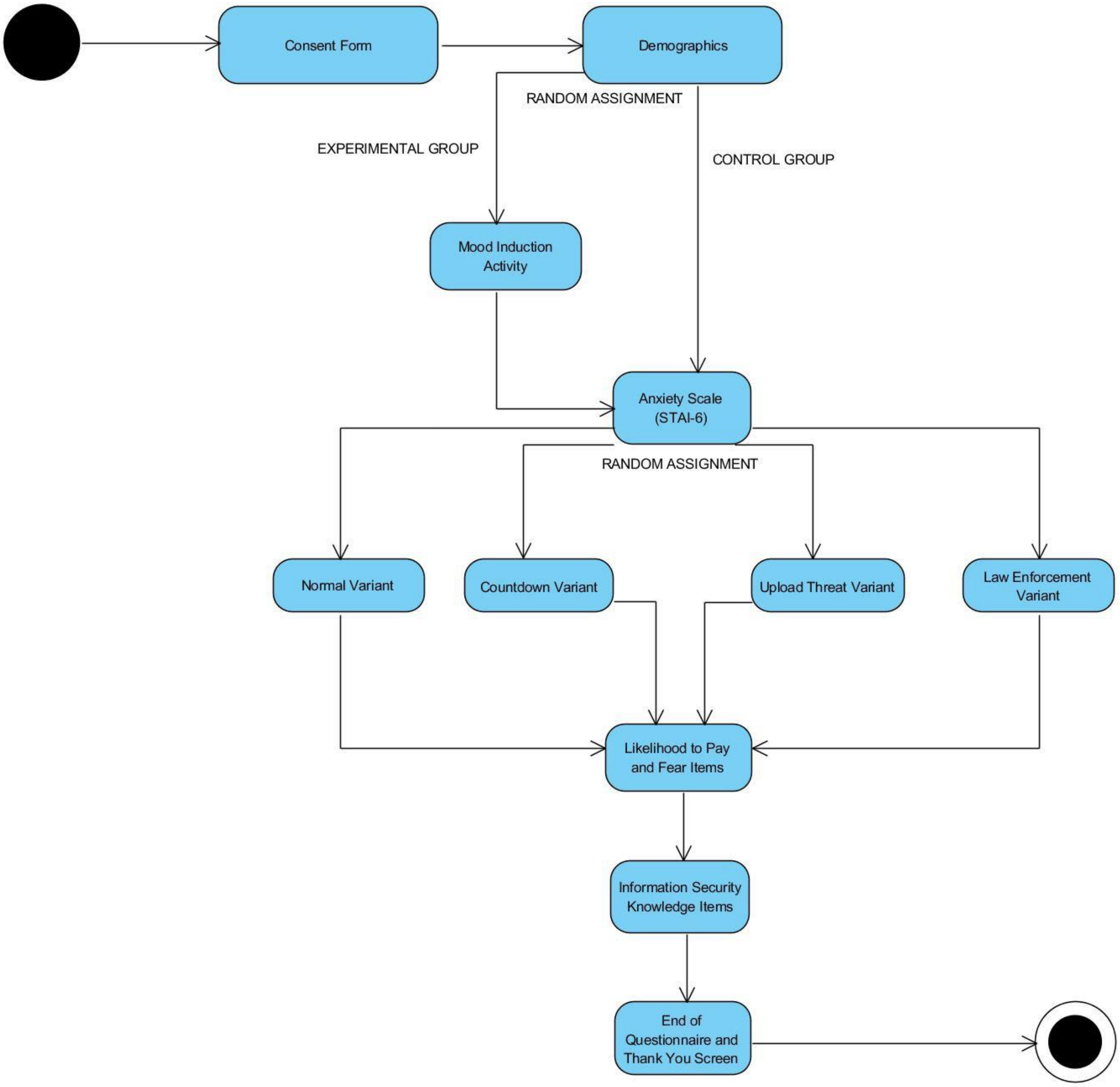


Figure 3.1. Survey methodology flowchart

Following these questions, the survey assigned participants to one of four ransomware vignettes. Participants were subjected to one of four variants: the normal (control) variant, the countdown clock variant, the law enforcement variant, and the upload threat variant. Each of these was labeled with directions to participants instructing them to imagine themselves experiencing the attack and to answer as if it were an actual attack. This was assigned randomly by Qualtrics. After 60 seconds to allow participants to react, the next set of questions was displayed. Participants were reminded what they saw was just a simulation but to answer according to how they felt when they saw the screen. Participants were assessed on their likelihood to pay and their knowledge with information security. Participants who indicated unwillingness to pay were asked what steps they would take next (such as asking a friend for help or contacting law enforcement). The vignettes were created in Adobe Photoshop using royalty-free assets. These vignettes were created based on the most common verbiage and characteristics from the literature and recent ransomware attacks.

Survey items not related to the ransomware were adapted from Anwar et al. (2017)'s study of cybersecurity behavior. This scale measures feelings towards information security behavior, as well as adherence to these policies. Likert-scale items were adapted from this study, which measure the following concepts: prior experience with computer security practices, security self-efficacy, peer behavior, and self-reported cybersecurity behavior.

Reliability analysis was performed on the four information security scales as well as the anxiety scale to ensure internal consistency. The information security scales comprised of four scales measuring prior behavior (α = .78), peer behavior (α = .83), self reported security behavior (α = .83), and self efficacy (α = .89). The cronbach's alpha for the six-item anxiety measurement was .86. This indicated all scales used in this study had sufficient internal consistency. A correlation between items of the same scales showed no issues with multicollinearity (Field, 2009).

Once these items were complete, participants were redirected to a screen explaining the purpose of the study and thanking them for their participation. Responses were recorded by Qualtrics and stored for analysis. No personally identifiable information was collected upon submission of the survey. Analysis was performed to discover which ransomware variants users are liable to pay.

3.3 Sample

This study sampled individuals over the age of 18 in the United States. After IRB approval (Protocol 1901021495), Participants were recruited online using Amazon's Mechanical Turk (Mturk). Mturk is a task recruitment site commonly used by researchers to recruit study participants, especially for survey-based research (Fleischer et al., 2015). Mturk can produce high-quality data with good generalizability (Arditte, Çek, Shaw, & Timpano, 2016; Behrend, Sharek, Meade, & Wiebe, 2011). Research has also shown Mturk data is valid and reliable (Goodman, Cryder, & Cheema, 2013). The site has users spread across the United States from a wide variety of demographics. Using Mturk, participants received 40 cents for their attentive response. This amount was chosen because this survey is short, and lower amounts are appropriate for shorter survey (Work, 2011). A total sample of N = 500 was recruited for this study. This number was chosen in order to have a sufficient n in each potential group. The participants were initially designated into one of two groups - the control group and the treatment group. Following this split, participants in each group were then assigned to one of the four variants. This resulted in 8 total groups, with around n = 60 each. This number was large enough to allow cleaning of responses and removal of any incomplete or invalid responses. This was a random assignment.

3.4 Procedure

This anonymous survey was first piloted before being posted to Mturk in order to test survey flow and to receive feedback on each item. A survey was chosen as the methodology for recording and collecting data because data can be collected quickly and immediately anonymized. A business owner, for example, may wish to report they would never pay the ransom in an attack, even if they believe they would, in order to maintain their appearance. This phenomenon is known as response bias. Marquis, Marquis, and Polich (1986), in their study of response bias, found surveys an acceptable tool with regards to response bias; participants did not seem to withhold their responses.

Individual responses were not be published, nor was any identifying information, so it is anticipated participants were honest. Online surveys are most appropriate for individuals familiar with the use of technology (Shannon, Johnson, Searcy, Lott, et al., 2002). As this study requires participants to own a personal device, this should not be a concern. A mood induction activity also helped decrease response bias, encouraging participants to respond emotionally.

Another threat to validity with a survey is inattentive responding. Participants may become bored or wish to finish the survey quickly and fail to read the questions completely. Inattentive responding can be a larger threat with online surveys (Fleischer et al., 2015). There were methods included in this research to decrease this effect. Since participants have willingly agreed to participate in this research, it is expected they paid attention more than an average mass-distributed online survey. Couper, Kapteyn, Schonlau, and Winter (2007) found if participants indicated prior willingness to complete an online survey, they are likely to follow through with it. In addition, an attention check question was included. The attention check question instructed participants to pick a specific option regardless of the question itself; if users failed this question, they were disqualified and not included in the final analyses.

As ransomware is damaging and puts personal data at risk, it was necessary to simulate the attack using a vignette. It would not be possible or ethical to install a true ransomware attack onto a participant's device. Participants were likely only to feel any real attachment to the data if the study was done on their own device, containing their own personal data, which is why a lab machine or virtual machine was not utilized. Participants were likely to realize the attack was a simulation and fail to respond truthfully to how they would respond to a real attack. Therefore, care was taken to ensure all participants are in a state of heightened emotion and anxiety.

Pacheco-Unguetti, Acosta, Callejas, and Lupiáñez (2010) found higher levels of anxiety altered decision-making ability. As an individual will likely experience high anxiety and stress during a real ransomware infection, it was desirable for participants to feel similar during this research, even if they suspect it is a simulation. Their decisions of whether or not to pay can be altered by their emotional state. Another study by Jung, Wranke, Hamburger, and Knauff (2014) was conducted in which participants were given various logic and calculation puzzles. Participants were then put under mood induction procedures and given more puzzles. The authors found:

> The results indicate that the emotions of an individual have an effect on reasoning performance independent from task content. In particular, a negative emotion resulted in a lower falsification index meaning that participants in a negative emotional state were more likely to deviate from logical norms (p. 5).

This study followed a similar design.

3.5 Analytical Methods

Once data had been collected in Qualtrics, it was exported for analysis. The STAI-6 score was scored along with the cybersecurity behavior scales and response to the ransomware. First, a *t*-test was performed on the STAI-6 score for both the experimental group and the control group. This determined whether the mood induction activity had an effect (see Manipulation Check).

After the manipulation check, the hypotheses were tested. The first hypothesis was tested using a 2 x 4 factorial ANOVA with robust estimations and two one-way ANOVAs. These were employed to resolve issues with homogeneity of variance.

The second hypothesis was tested by first performing a partial correlation between the information security scales and each measurement of likelihood to pay, controlling for anxiety. This ensured the difference for the experimental and control group was taken into account. This correlation showed if the score on each scale was associated with paying or not paying the ransom. A linear regression was also considered, but issues with homogeneity of variance meant assumptions for this test were not met. The Hosmer-Lemeshow test, a test for goodness of fit, was significant at $p = .001$. This indicates the data would not be a good fit for a regression (Field, 2009).

3.5.1 Manipulation Check

Since participants in the experimental group were exposed to a mood induction procedure, it was necessary to perform a manipulation check in order to determine whether the mood induction had the desired effect of inducing anxious mood. A *t*-test analyzed difference on average between the experimental and control group after the mood induction for the anxiety scale. A *t*-test showing anxiety scores differing at $p < .05$ indicated the mood induction had an effect.

3.5.2 Summary

This chapter explained the hypotheses the author aimed to answer and the support for employing the resulting methods. In order to collect data, an anonymized survey was posted to Amazon’s Mturk site. Once collected, data was analyzed in accordance with the proposed methods in IBM’s SPSS statistical software. The survey contained questions regarding likelihood to pay, and participants were randomly put into an experimental and control group; the experimental group experienced a mood-induction activity to ensure participants were in a mood similar to what they would be in during a real attack.

CHAPTER 4. RESULTS

Analysis was performed in IBM SPSS Statistics Version 25. SPSS is a commonly used software package for statistical analysis. Data was exported from Qualtrics in SPSS format upon completion. The demographics of the resulting dataset are described, and the results of the manipulation check are expressed. The final analyses conducted to test the hypotheses are shown, as well as issues with homogeneity of variance were addressed. Finally, *post hoc* analyses were performed and described on some of the additional questions asked, such as why users did not pay.

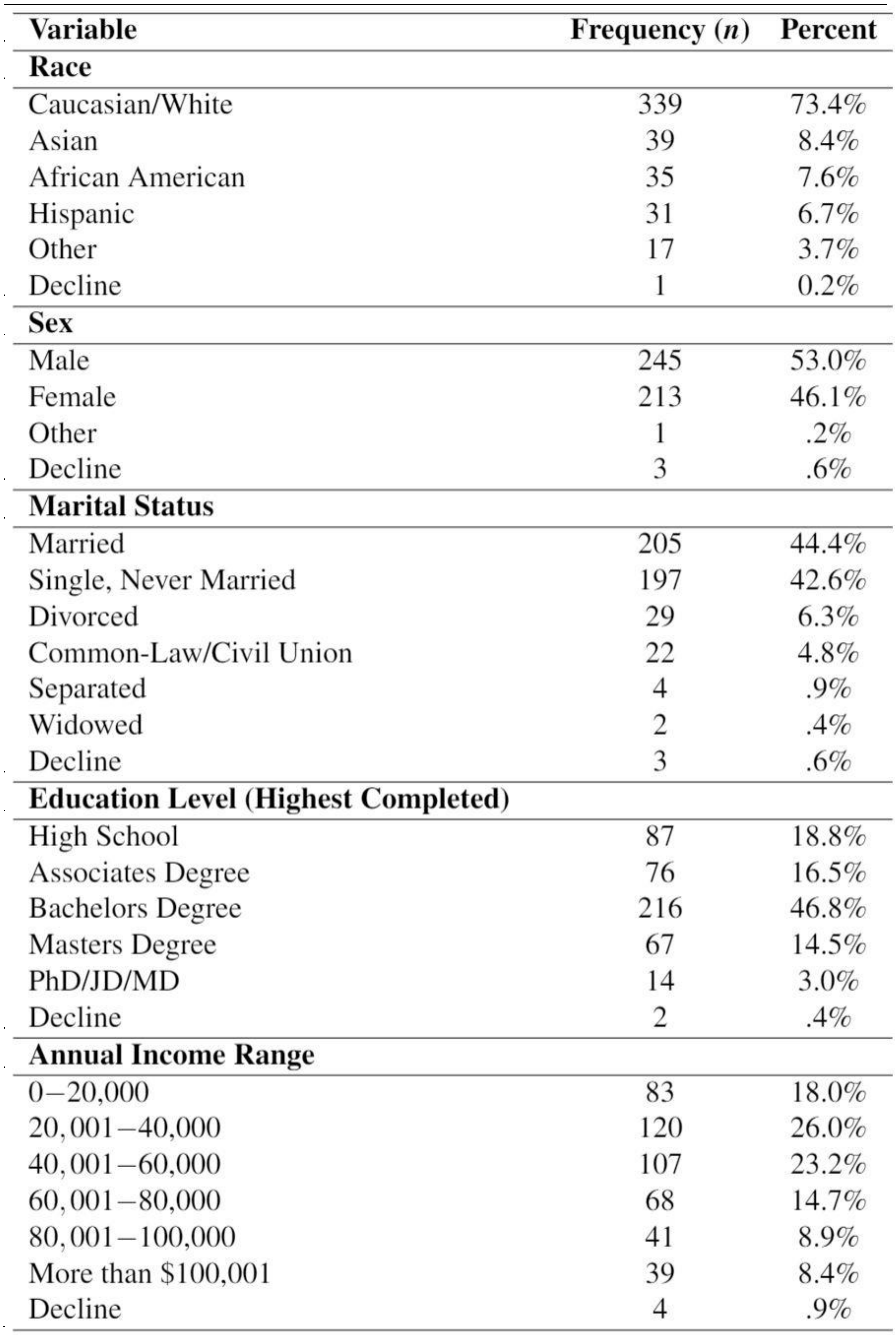
4.1 Manipulation Check

Induction of anxiety was verified using an independent-sample *t*-test. Results of the manipulation check showed participants exposed to the mood induction activity (M = 2.04, SD = .79) reported a higher level of anxiety than those who were not exposed to the activity (M = 1.68, SD = .71). This difference was significant at $t(460) = -5.14$, $p < .001$; which showed the anxiety-inducing activity was successful as the experimental group reported higher anxiety, on average, than the control group.

4.2 Descriptives

In total, 838 responses were recorded in Qualtrics. Once imported into SPSS, data was analyzed for unusable or invalid data. Participants who did not provide consent on the consent form, reported being under 18, or did not currently live in the United States were considered invalid responses. In addition, any participant who failed the attention check question was also considered invalid, as there is no way to verify whether they took the survey seriously or provided accurate responses to the remaining questions.

Table 4.1. Demographic information



Variable	Frequency (*n*)	Percent
Race		
Caucasian/White	339	73.4%
Asian	39	8.4%
African American	35	7.6%
Hispanic	31	6.7%
Other	17	3.7%
Decline	1	0.2%
Sex		
Male	245	53.0%
Female	213	46.1%
Other	1	.2%
Decline	3	.6%
Marital Status		
Married	205	44.4%
Single, Never Married	197	42.6%
Divorced	29	6.3%
Common-Law/Civil Union	22	4.8%
Separated	4	.9%
Widowed	2	.4%
Decline	3	.6%
Education Level (Highest Completed)		
High School	87	18.8%
Associates Degree	76	16.5%
Bachelors Degree	216	46.8%
Masters Degree	67	14.5%
PhD/JD/MD	14	3.0%
Decline	2	.4%
Annual Income Range		
0−20,000	83	18.0%
20,001−40,000	120	26.0%
40,001−60,000	107	23.2%
60,001−80,000	68	14.7%
80,001−100,000	41	8.9%
More than $100,001	39	8.4%
Decline	4	.9%

To remove these cases, a new variable was created with a default value of zero. Any participant considered invalid had this variable set to one. These cases were then removed from the dataset, which comprised of 357 cases. In addition, 19 individuals were removed for inattentive responding, such as responding “prefer not to respond” for every question. After removal of these cases, a total of 462 cases remained. As shown in Table 4.1, 53% (*n* = 245) of survey respondents were male, while 46.1% (*n* = 213) were female. Most participants identify as Caucasian (*n* = 339, 73.4%). Most participants were either single (*n* = 197, 42.6%) or married (*n* = 205, 44.4%). The most common level of education achieved was a bachelor’s degree (*n* = 216, 46.8%).

4.2.1 Scale Items

All scale items were scored using aggregate statistics to provide an average score. The six-item anxiety scale as well as each block of information security questions (measuring self-reported behavior, peer behavior, prior knowledge, and self-efficacy) were averaged across the items to provide a value for each construct. Each concept was, thus, given an average score for each participant. Because the scales were calculated via the mean, participants were allowed to miss one question and still be given a score.

4.3 Hypothesis Testing

H_1: Individuals will report a higher likelihood to pay when exposed to ransomware with scare tactics.

The factorial ANOVA’s assumptions were not met as Levene’s test was significant (*F* = 6.94, $p < .001$). As a result of Levene’s test being violated, equality of variances cannot be assumed. Two methods were employed to account for this assumption not being met. The first method was to use a robust parameter estimate adjustment to the factorial ANOVA, which assisted in achieving a measure of the interaction between the two groups. This method is recommended when analyzing data with unequal variances in SPSS (IBM, n.d.). The interaction between the control group and the law enforcement variant was significant (*B* = -.82, *p* = .015), meaning those in the control group were less likely to pay the law enforcement variant compared to all other types.

The second method was to perform two individual one-way ANOVAs for each group (i.e. experimental condition and type of ransom on whether a respondent will pay or not). This allowed the use of the Welch statistic as well as the Games-Howell test, which are robust when homogeneity of variances is violated. Levene's test was still significant ($p < .05$) for both one-way ANOVAs. There was a significant effect of type of ransomware on likelihood to pay, Welch's $F(3, 251.36) = 2.67$, $p = .048$. This finding represents a small effect size between type of ransomware on likelihood to pay, $\omega = .0121$. *Post hoc* tests revealed receiving the law enforcement variant resulted in a marginally significant decreased likelihood to pay compared to the default variant (Games-Howell, $p = .051$). There was no significant mean difference between any of the other ransomware types on likelihood to pay. There was also no significant effect of the experimental group on likelihood to pay, Welch's $F(1, 405.83) = .052$, $p > .05$.

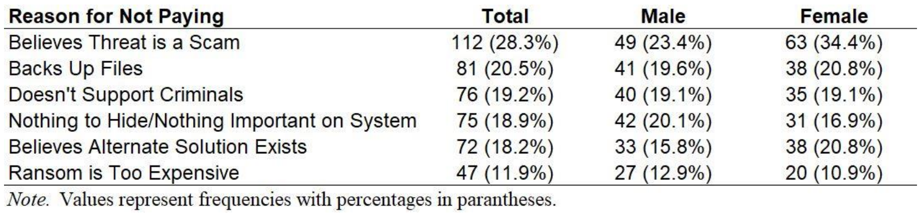
Overall, this hypothesis was not supported. Participants did not show a higher likelihood to pay when exposed to scare tactics. Being exposed to the law enforcement variant resulted in a decreased likelihood to pay, and the other variants did not show a significant effect.

H_A: Familiarity with secure computer and internet behaviors will decrease likelihood to pay the ransom in participants.

The first step taken to test this ancillary hypothesis was a one-tailed partial correlation, controlling for anxiety. When controlling for anxiety on the relationship between likelihood to pay the ransom and self-reported information security behavior, there was a moderate negative correlation $r = -.21$, $p < .001$. However, both peer behavior ($r = .15$, $p = .001$) and prior experience ($r = .19$, $p < .001$) were positively correlated with paying the ransom. When forced to make a decision on payment (yes or no), two of these relationships remain, with prior experience ($r = .12$, $p = .006$) and self reported behavior ($r = -.18$, $p < .001$) still being significantly correlated. A full intercorrelation table can be found in Table 4.4.

Results indicated as peer behavior and prior experience behaviors increase, the likelihood of an individual to pay the ransom also increases. Self-reported information security behavior may be associated with a decrease in likelihood to pay the ransom. Overall, this hypothesis was only partially supported. When forced to make a decision, one information security scale (self-reported information security behavior) was correlated with a decreased likelihood of payment. However, two of the scales showed no effect, and prior experience was positively correlated with payment.

Table 4.2. Reasons for not paying ransom



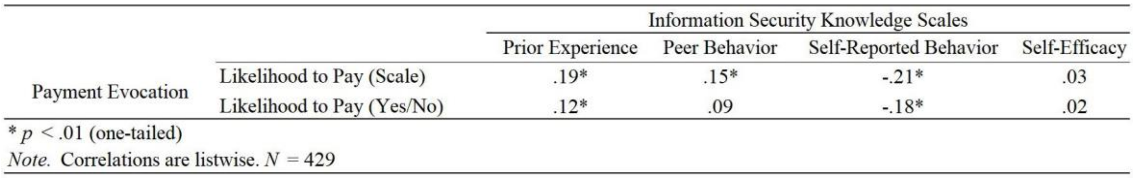
Reason for Not Paying	Total	Male	Female
Believes Threat is a Scam	112 (28.3%)	49 (23.4%)	63 (34.4%)
Backs Up Files	81 (20.5%)	41 (19.6%)	38 (20.8%)
Doesn't Support Criminals	76 (19.2%)	40 (19.1%)	35 (19.1%)
Nothing to Hide/Nothing Important on System	75 (18.9%)	42 (20.1%)	31 (16.9%)
Believes Alternate Solution Exists	72 (18.2%)	33 (15.8%)	38 (20.8%)
Ransom is Too Expensive	47 (11.9%)	27 (12.9%)	20 (10.9%)

Note. Values represent frequencies with percentages in parantheses.

Table 4.3. Payscale frequencies for ransom amounts

Ransom Amount	**Default**	**Law Enforcement**	**Upload**	**Countdown**	**Total**
$1-100	21	18	18	22	79
$101-200	15	5	4	12	36
$201-300	10	1	3	13	27
$301-400	8	1	3	6	18
$401-500	10	4	4	7	25
$501-600	9	1	3	7	20
$601-700	5	0	2	4	11
Over $1000	9	1	2	3	15

Table 4.4. Partial correlation



		Information Security Knowledge Scales			
		Prior Experience	Peer Behavior	Self-Reported Behavior	Self-Efficacy
Payment Evocation	Likelihood to Pay (Scale)	.19*	.15*	-.21*	.03
	Likelihood to Pay (Yes/No)	.12*	.09	-.18*	.02

* p < .01 (one-tailed)

Note. Correlations are listwise. N = 429

4.4 *Post hoc* Tests

When forced to make a decision, the majority of respondents (*n* = 216, 87.7%) chose to not pay the ransom. Only 12.3% (*n* = 57) chose to pay. Respondents were asked to describe in an free-response box why they did or did not pay the ransom. Categories describing these responses were created by two researchers reviewing the data to look for common themes and concepts; two researchers were utilized to increase inter-rater reliability. Responses were allowed to fall into multiple categories, as many participants expressed multiple sentiments in one response; these cases of multiple reasons are also expressed in the table totals. If researchers disagreed on an individual category, the response was not included in that individual reason's count, but the response would remain counted in other agreed upon categories. In accordance with the method developed by Landis and Koch (1977), an interrater reliability analysis using the Kappa statistic was performed to determine consistency among raters. This analysis showed almost perfect agreement among raters. Based on the responses, there were six main reasons (dichotomous - yes or no) respondents chose not to pay: (1) the respondent does not wish to support criminals (Kappa = .96, $p <$ .001), (2) the respondent already has files backed up (Kappa = .94, $p <$ .001), (3) the respondent believes the threat was a scam (Kappa = .94, $p <$ .001), (4) the respondent believed the ransom was demanding too much money (Kappa = .97, $p <$ .001), (5) the respondent has nothing important and nothing to hide on their system (Kappa = .94, $p <$ .001), and (6) the respondent believes there is an alternative way to fixing the issue (Kappa = .91, $p <$ .001) (see Table 4.3). Of the reasons, believing the threat was a scam was the most common (*n* = 112, 28.3%), while the ransom being too expensive was the least common (*n* = 47, 11.9%).

The reasons for not paying a ransom varied by demographic group. For example, 10.6% of participants who made between $20,000 - $40,000 per year indicated cost as a factor, while only 4.3% of those who made over $100,001 per year indicated the ransom was too expensive. In addition, those with advanced degrees appeared to believe they could find an alternate solution to paying the ransom, with 28.6% of respondents with a PhD/JD/MD responding in this manner.

Next, those who did not pay the ransom were asked their likelihood to take some next steps. The most likely next step was to ask a more computer-knowledgeable individual (such as a friend or family member) for help, with 73.8% (*n* = 297) indicating they were either likely or very likely to pursue this option. The next most popular option was to contact law enforcement, with 57.6% indicating either likely or very likely for this choice. It was almost equally as likely for individuals to contact a technical support line (*n* = 207, 52%) as it was to taking their computer to an IT help desk, such as Geek Squad (*n* = 208, 52.2%).

The least likely option was to take no further action due to data already being backed up, with 46.1% (*n* = 182) indicating this option as likely or very likely.

Finally, a cross-tab of ransomware type and payment amount was generated in Table 4.3. The number in each box indicates the number of people willing to pay at each amount. Participants were instructed to check each box they would be willing to pay. In general, participants appeared to pay each ransom type equally at low amounts, but at higher amounts, the default ransom was the most commonly paid option.

CHAPTER 5. DISCUSSION

The aim of this study was to examine payment evocation in different variants of ransomware and what contributed to this payment evocation, including the variants as well as knowledge of information security amount participants. This study took place anonymously online using Amazon's Mturk. The results were analyzed to determine which factors contributed to ransomware payment evocation. In addition, *post hoc* tests were performed to examine additional questions from the study, including differing levels of price as well as next steps an individual would take after receiving a ransom message.

The responses from participants showed the majority of individuals (*n* = 216, 87.7%) did not choose to pay the ransom when forced to make a yes or no decision. This is a useful finding because it could indicate the general population may not know the dangers of ransomware, or they already have adequate protection. Not knowing the dangers of ransomware could be a costly mistake for many individuals as shown by studies such as Brewer (2016) and Liao et al. (2016).

Thus, to help discover why the majority did not choose to pay, an analysis was performed on the free response question asking participants why they chose not to pay. Of note was the large amount of participants who reported they did not believe the ransom message, instead believing it was a scam (*n* = 112, 28.3%). Ransomware is a well-known threat with many variants which do follow through on its promise to lock files (O'Gorman & McDonald, 2012). The only variant which typically does not follow through is the upload variant, although it still does lock files, only failing to actually follow through with the threat to upload files to a server (Malwarebytes, 2016). This could indicate a need for user education. If users in an organization do not believe ransomware is a true threat, they may not take the proper precautions or react in a serious and timely manner when a system is infected.

A potential area for user education is the relatively low amount of individuals reporting proper backups as a reason for not paying the ransom. In the text response, few individuals (*n* = 81, 20.5%) mentioned backing up their system as a reason to not pay. In the likert-scale option, less than half (*n* = 182, 46.1%) indicated having their system backed up as a likely or very likely option for not paying the ransom. A model created by Caulfield et al. (n.d.) has shown in the general population, it would likely take 70% of the population backing up their systems regularly to make ransomware an unprofitable business. If more users knew ransomware is a real threat, and that backing up is an effective preventive measure, it may be possible to reach that 70% figure in the future. In addition, the type of backup will play a role in whether users are truly protected or not. Users may choose to upload their backup data to their local storage, a cloud service, or an external device. Some ransomware is able to infect local storage, if the drive is mapped to be accessible on the infected machine. Cloud storage could potentially be affected if the ransomware is designed to attack that service provider and the user has not restricted access. Therefore, care must be taken to ensure users are trained on proper backup options which will be effective against ransomware. This also has a financial consideration for businesses. Backup solutions are an important cost-benefit decision when applied to business customers (Alhazmi & Malaiya, 2013). Businesses may have to make an economic decision between paying for a robust solution and accepting the potential payment of a ransom.

Another finding of the study was the variant of ransomware did not have a large effect on payment, and the law enforcement variant resulted in the least amount of participants choosing to pay. This may be because participants were skeptical of the legitimacy of the threats provided. While the law enforcement variant of ransomware is not truly from a law enforcement agency, it still does pose a threat, as it locks and holds files ransom just as any other variant, making it just as dangerous. Users should be reminded that while the threat of arrest is not true, the financial risk is just the same. This helps display why preventive measures such as antivirus and proper backups are so important; regardless of the trustworthiness of the scare tactic, the software is still damaging. Users should be trained to prevent against all variants, even if the threats don't seem legitimate.

A misconception found in the study is many people believe another entity (such as an IT help desk or law enforcement) will be able to remove the ransomware. In the text response, 18.2% (*n* = 72) believed an alternate solution existed that could remove the ransom without payment. While this is true for some ransomware, this is not the norm. A majority (73.8%, *n* = 297) indicated their next step would be to ask for help from a more computer knowledgeable individual. This could indicate ransomware is not a well-known threat in the general population. Perhaps individuals would be more proactive and know how to respond if they understood the threat prior to an attack. While many computer users use antivirus software (AV-Comparitives, 2019) and are familiar with basic viruses, they may not understand ransomware's particularly destructive threat. This is vital information to correct when individuals go to work, as ransomware is one of the most common worries small-to-medium sized business owners report (Lab, 2016). While this study did not focus on business users as a unit of interest, individuals in the general population go to work. Whether their business is a small or large institution, that business could be devastated if a ransomware attack occurred. If their employees do not take a threat like ransomware seriously, the entire business network could be at risk. This is not a hypothetical situation, as hospitals received over 24 ransomware attacks in a six month period (Mansfield-Devine, 2016). This is a non-trivial threat for individuals as well, as without a backup, individuals can lose financial documents, personal photos and memories, and anything else of value on their system. While other viruses can often be removed with an antivirus program after-the-fact, this is not always the case with ransomware, regardless of how computer-savvy the individual assisting is.

A surprising result of the study was two information security knowledge factors (prior experience and peer behavior) were positively correlated with paying the ransom. While studies such as Luo and Liao (2007) demonstrate the importance of awareness, it is possible participants with prior experience in information security know the threat is legitimate, and that often the only option is to pay. As discussed earlier, many participants simply discarded the threat as a scam. Similarly, with peer experience, an individual may know a coworker or friend who has been forced to pay a ransom after an attack. When this is taken into account, the finding is not unreasonable. Future studies could look at how familiarity with ransomware itself plays a role in the decision to make a final payment, and what steps those with knowledge of ransomware have taken to protect themselves.

Another factor to take into consideration is demographics and the ability of an individual to pay a ransom given their socioeconomic status. 43% (*n* = 203) of participants indicated their annual income was $40,000 or less. For these individuals, paying a ransom of $1000 could be cost restrictive. Those at higher income levels may find it more of a convenience to pay the ransom than to try to recover the files manually or deal with losing them. Individuals may be responsive at a lower price. While the default was set at $1000, previous ransomware attacks have shown that attackers are occasionally willing to bargain with those who cannot afford the ransom price (Hernandez-Castro et al., 2017). Because of this, participants were asked to rate some lower amounts and their likelihood to pay. As prices became lower, more participants reported they would pay the ransom. This could have a broader impact for businesses, whose ransom demands could potentially exceed into the millions. Businesses should have contingencies for when their preventive measures fail, as it will become necessary to determine whether paying the ransom amount is worth it when taking into account the amount of financial damage caused by the data loss. In addition, there is an ideological component to consider. Ransomware attackers are criminals, and 19.2% (*n* = 76) of participants indicated not supporting criminals as a reason for not paying the ransom. While not paying the ransom may cause a greater financial loss, paying ransoms contributes to their future success; this is a factor many take into account.

5.1 Limitations

A limitation of this study is the inability to capture a user's true emotional response from attack to final decision during a real attack. It is possible a participant reported they would never pay a ransom, but if actually in the situation, would decide to do so in order to recover their files. However, this would be a difficult study to conduct, as placing ransomware on a participant's device would be destructive and illegal.

Another limitation of this study is the low amount of participants who chose to pay. This made analysis difficult because the data was skewed and lacked homogeneity of variance. A larger dataset may have been able to correct for this. It also may be worth conducting this study with business users as the target audience in the future. Businesses often have ransomware as a major concern due to the amount of potential data loss, and as a result, business users may report willingness to pay at a higher rate than the general population.

Demographics and culture may also play a role in why a user may choose not to pay a ransom. This study recruited only residents of the United States; some participants expressed that it is an American value to not support terrorists or other malicious actors. Those in other countries may express different values or assess different meaning to the data on their device. As discussed earlier, income also plays a role. This may be more relevant in developing countries where the median personal income is lower.

5.2 Conclusion

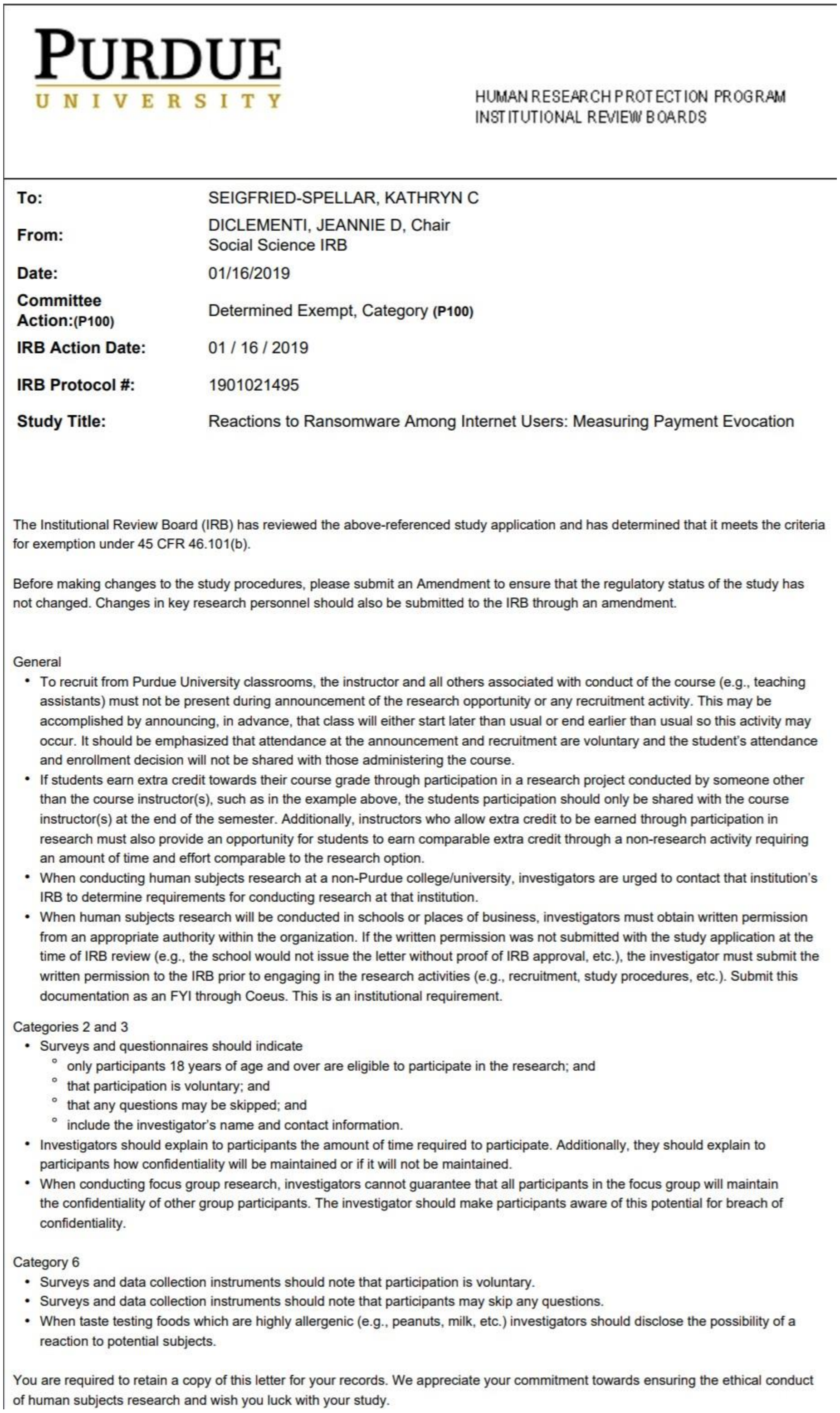
Ransomware is a growing threat among modern malware due to its resilience to antivirus software, and often the only way to recover lost data is paying the ransom. The widespread success of ransomware attacks and off-the-shelf ransomware has allowed criminals to exploit a large amount of people. This study surveyed the general population to discover which type of ransomware was most likely to evoke payment as well as whether knowledge of information security had an effect on this payment evocation. Most individuals did not choose to pay the ransom. Based on the statistical analysis performed in this study, this lack of payment can be attributed to a large amount of participants believing ransomware is a scam or not wanting to support criminals. Not believing the ransom threat can be problematic, and more training should be implemented to ensure the population understands the irreversible nature of most ransomware and the importance of prevention and backups. This is especially vital to businesses and enterprises who rely on their employees to not fall victim to these attacks and take prevention methods seriously.

There are multiple angles for future research in this area. As mentioned prior, business users would be another suitable population for this study due to the unique constraints and importance of data of business and enterprise units. Business decisions would also be affected by backup infrastructure and economic resources. This would provide another gauge for a major vulnerable population and their preparedness for an attack.

Another future area of research is to delve further into the reasons for nonpayment. Having proper backups was one of the least expressed possibilities, and in an ideal world, this would be the most popular option. There may be other reasons not expressed in this study why participants did not trust the ransom. For example, the method of payment

(Bitcoin, MoneyPak, etc.) may play a role, especially in regards to trusting the message. Further investigation could be done regarding the ransom amount, especially as it relates to the socioeconomic bracket an individual falls into. Finally, as with all types of cybercrime, ransomware is constantly evolving and changing. New variants will more than likely be identified every month, and research could be conducted on future variants, especially as attackers develop newer and more complex scare tactics.

APPENDIX A. IRB EXEMPTION



PURDUE
UNIVERSITY

HUMAN RESEARCH PROTECTION PROGRAM
INSTITUTIONAL REVIEW BOARDS

To:	SEIGFRIED-SPELLAR, KATHRYN C
From:	DICLEMENTI, JEANNIE D, Chair Social Science IRB
Date:	01/16/2019
Committee Action:(P100)	Determined Exempt, Category **(P100)**
IRB Action Date:	01 / 16 / 2019
IRB Protocol #:	1901021495
Study Title:	Reactions to Ransomware Among Internet Users: Measuring Payment Evocation

The Institutional Review Board (IRB) has reviewed the above-referenced study application and has determined that it meets the criteria for exemption under 45 CFR 46.101(b).

Before making changes to the study procedures, please submit an Amendment to ensure that the regulatory status of the study has not changed. Changes in key research personnel should also be submitted to the IRB through an amendment.

General

- To recruit from Purdue University classrooms, the instructor and all others associated with conduct of the course (e.g., teaching assistants) must not be present during announcement of the research opportunity or any recruitment activity. This may be accomplished by announcing, in advance, that class will either start later than usual or end earlier than usual so this activity may occur. It should be emphasized that attendance at the announcement and recruitment are voluntary and the student's attendance and enrollment decision will not be shared with those administering the course.
- If students earn extra credit towards their course grade through participation in a research project conducted by someone other than the course instructor(s), such as in the example above, the students participation should only be shared with the course instructor(s) at the end of the semester. Additionally, instructors who allow extra credit to be earned through participation in research must also provide an opportunity for students to earn comparable extra credit through a non-research activity requiring an amount of time and effort comparable to the research option.
- When conducting human subjects research at a non-Purdue college/university, investigators are urged to contact that institution's IRB to determine requirements for conducting research at that institution.
- When human subjects research will be conducted in schools or places of business, investigators must obtain written permission from an appropriate authority within the organization. If the written permission was not submitted with the study application at the time of IRB review (e.g., the school would not issue the letter without proof of IRB approval, etc.), the investigator must submit the written permission to the IRB prior to engaging in the research activities (e.g., recruitment, study procedures, etc.). Submit this documentation as an FYI through Coeus. This is an institutional requirement.

Categories 2 and 3

- Surveys and questionnaires should indicate
  - only participants 18 years of age and over are eligible to participate in the research; and
  - that participation is voluntary; and
  - that any questions may be skipped; and
  - include the investigator's name and contact information.
- Investigators should explain to participants the amount of time required to participate. Additionally, they should explain to participants how confidentiality will be maintained or if it will not be maintained.
- When conducting focus group research, investigators cannot guarantee that all participants in the focus group will maintain the confidentiality of other group participants. The investigator should make participants aware of this potential for breach of confidentiality.

Category 6

- Surveys and data collection instruments should note that participation is voluntary.
- Surveys and data collection instruments should note that participants may skip any questions.
- When taste testing foods which are highly allergenic (e.g., peanuts, milk, etc.) investigators should disclose the possibility of a reaction to potential subjects.

You are required to retain a copy of this letter for your records. We appreciate your commitment towards ensuring the ethical conduct of human subjects research and wish you luck with your study.

APPENDIX B. IRB NARRATIVE

PROPOSED RESEARCH RATIONALE

This study is designed to investigate which variant of ransomware is most likely to evoke payment from people and whether previous knowledge of secure computing behavior affects this response.

B. SPECIFIC PROCEDURES TO BE FOLLOWED

Participants will be recruited through Amazons Mechanical Turk (MTurk) website. If an MTurk worker (i.e., potential study participant) wishes to complete this study, he/she will be provided with a link to Purdue Universitys Qulatrics website where the study will take place. The opening page of the survey will include the Informed Consent. If the respondent chooses to continue, the rest of the study will be administered. This consists of a demographics form, which includes questions about age and permanent residency. If the participant is under 18 or is not a permanent resident of the US, he/she will not be allowed to continue. Following the consent form, participants will be assigned into the control group and experimental group. The experimental group will go through a puzzle activity to induce anxiety. The activity will consist of a puzzle of increasing difficulty. After this, both groups take an anxiety inventory and are presented with one of four ransomware vignettes. No actual malware will be installed or downloaded on any device. After the vignette, questions will be presented regarding likelihood to pay the ransom. Next, participants will take an inventory asking about information security knowledge and behavior.

After this questionnaire, a final page is presented that thanks the participant and instructs him/her to Please use the following code words to receive payment: Boiler Up. A respondent would then return to the MTurk solicitation page and enter Boiler Up into the text box. The researcher would then be notified, via email, that a respondent completed the survey. If the respondent enters the correct code words the researcher will pay them through the anonymous account. If the participant enters an incorrect code words (e.g., Go Hoosiers), the researcher will be alerted that the participant did not complete the study and will select the do not pay option. If the respondent misspells the code (Bolier Up) or submits the code with a typo (Boiler Yp), the respondent will still be compensated for completing the study. Consistent with pricing of other surveys on MTurk, participants will be paid $0.40 for completing the study. No identifying information will be collected; this survey will be completely anonymous. The State-Trait Anxiety Inventory (STAI-6) is a scale consisting of 6 likert-scale items measuring anxiety.

The information security inventory consists of 27 likert-scale items measuring experience with computer security practices, security self-efficacy, peer behavior, and self-reported cybersecurity behavior.

SUBJECTS TO BE INCLUDED Participants will be 500 men and women recruited through Amazons Mechanical Turk Website. Participants will be required to over the age of 18 and to be permanent residents of the United States.

D. RECRUITMENT OF SUBJECTS AND OBTAINING INFORMED CONSENT Respondents (N = 500) will be solicited from the website Amazon Mechanical Turk (MTurk). Research has demonstrated MTurk may be used to obtain high-quality data inexpensively and rapidly from a diverse participant pool (Buhrmester, Kwang, and Gosling (2011) and provides better generalizability than snowball sampling procedures (c.f., Berinsky, Huber, & Lenz, 2011). A solicitation for study participation will be posted to the MTurk website by the Primary Investigator, Dr. Seigfried-Spellar. This solicitation will include a survey link that respondents can click on if they are interested in participation. This link will direct them to Purdue Universitys Qualtrics website, where the entirety of study procedures will take place. The opening page of the Qualtrics survey will include the Informed Consent (see Attachment: Informed Consent). If respondents choose to proceed with participation, they will click on the survey link and be directed into the survey. There will be no direct or indirect contact between researchers and potential participants. No identifying information will be collected. The consent form will state that only individuals 18 years of age and older AND permanent residents in the United States will be able eligible to complete the study. In addition, the demographics questionnaire will specifically ask the respondents to identify their current age and permanent residence any individual who is not 18 years of age or older AND a permanent resident of the US will be screened out of the study and not eligible for compensation.

E. PROCEDURES FOR PAYMENT OF SUBJECTS In line with current pricing practices on MTurk, participants will be paid $0.40 for completing the survey. The investigators deposit money with Amazon which pays participants directly.

F. CONFIDENTIALITY The study is completely anonymous. All data will be collected via an internet-based survey via Qualtrics. No identifying information will be collected, such as IP addresses or names. All payment is handled through Amazon.

A copy of the raw data will be downloaded from Qualtrics and stored on the PIs computer. This raw data will already be anonymous since no identifying information will be collected in the survey. The file will be saved in an encrypted format. Only the PI and Co-PI will have access to the encrypted file. The file will be kept for seven years according to APA standards.

G. POTENTIAL RISKS TO SUBJECTS The risks are considered minimal for this research; that is, they are no greater than everyday activities. The only potential risk will be the artificial anxiety produced by the mood induction activity. The activity is a puzzle consisting of increasing difficulty. While frustrating, this should not induce a large amount of distress. The study is anonymous. The only risk is breach of confidentiality in that the respondent tells someone that they completed the study; however, even then it will not be possible to link the responses back to an individual. The safeguards used to minimize this risk can be found in the confidentiality section.

H. BENEFITS TO BE GAINED BY THE INDIVIDUAL AND/OR SOCIETY There are no direct benefits to individuals completing the study. Potential benefits to society are small based on this study alone. There may be broader benefits to society to be had from the larger program of research. Understanding the human response to ransomware can help improve messaging and training regimens. Ransomware is a problem which cannot be solved by technical solutions alone in its current form, and expanding the body of literature to show which factors decrease payment evocation will benefit the security community as a whole.

I. INVESTIGATORS EVALUATION OF THE RISK-BENEFIT RATIO Risks are minimal, no greater than that encountered in daily life. There are, however, potential benefits of this research program.

J. WRITTEN INFORMED CONSENT FORM Submit a copy of an informed consent document in the form that it will be disseminated to subjects. If children are subjects, provide the Parental Consent Form, and, if appropriate, a Child Assent Form. If recruiting subjects who do not speak English, submit both an English version as well as a version translated into the appropriate language.

K. WAIVER OF INFORMED CONSENT OR SIGNED CONSENT The researchers request a Waiver of Signed Consent since this is an Internet-based study. Although there will be a consent form, the respondents will not be signing the online form but instead clicking Agree as an indication of their consent. The research study is completely anonymous and does not pose greater than minimal risk to general Internet users. Yes, the current study asks questions regarding deviant behavior so we want to make sure that this study is completely anonymous and does not record any identifiable information. No the current study does not require signed consent if in a non-research context. Yes, the respondents will still read a consent form, it will just be online, and they will indicate their consent by clicking on agree rather than signing their name.

L. INTERNATIONAL RESEARCH N/A

M. SUPPORTING DOCUMENTS (check all document that you will be submitting to IRB)

1. Informed Consent Form
2. Recruitment Materials
3. Demographics
4. Questionnair

APPENDIX C. IRB RECRUITMENT

MTurk Solicitation

MTurk requires certain fields to be filled in and are restricted by character count. The current study will include the following information based on MTurks standard solicitation page.

Title: Anonymous survey: Attitudes towards computer security

Brief Description: Give us your anonymous opinion on different types of computer behaviors, as well as certain aspects of information security.

Keywords: Anonymous survey, attitudes, security

Reward per assignment: $0.40

Qualifications Required: Location is US, 18 years of age or older

Anonymous survey: Attitudes towards computer security

You have the opportunity to be a part of research! Researchers from Purdue University are conducting an anonymous study on peoples attitudes toward computer behaviors as well as certain aspects of information security.

The study involves a short, anonymous survey. It will take approximately 15 minutes to complete. We will not be collecting any identifiable information (e.g., your name, IP address). Instead, your responses to the survey will be coded with a random ID number so we will not have to ask you for any personal information.

This HIT is periodically reposted; so if you have already completed this HIT previously, please do not complete it a second time. You will not be compensated a second time.

Anonymous Survey link: qualtrics.purdue.edu

In order to be compensated for completing this survey, please enter the special survey code here:

Thank You Web Page (Final Page of Study)

*Final page for those who successfully completed

study Thank you!

We appreciate you taking the time to be a part of research.

The purpose of this study was to gauge payment evocation after experiencing a ransomware attack, and to understand whether information security knowledge affects this response. The screens you saw were just simulations; no real malware has been installed onto your computer.

You may have been asked to complete a puzzle. This was used to increase anxiety and produce a mood more realistic to the one an individual would be in if exposed to a real ransomware attack on their device.

If you would like to learn more about ransomware and how to prevent it, please visit the following link:

https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-

cisos.pdf/view If you have any questions regarding this survey, you may contact

Dr. Kathryn

Seigfried-Spellar, the Principal Investigator, at XXXXXX@purdue.edu.

In order to receive compensation, please enter the following code into Mturk: ”_STUDY 2019 uUTCKp26̂3@auDCdXzU5”

Sorry Page

*Last page for respondents declined consent or screened out of survey because under 18 or not a US resident

Sorry, but based on one or more of your responses, you did not qualify for this study.

Thank you for your interest, and please contact the Principal Investigator if you have any questions: Dr. Kathryn Seigfried-Spellar at XXXXXX@purdue.edu

APPENDIX D. CONSENT FORM

Key Information

Please take time to review this information carefully. This is a research study. Your participation in this study is voluntary which means that you may choose not to participate at any time without penalty or loss of benefits to which you are otherwise entitled. You may ask questions to the researchers about the study whenever you would like. If you decide to take part in the study, you will be asked to sign this form, be sure you understand what you will do and any possible risks or benefits.

This study is designed to understand attitudes towards computer security and adherence to secure computing behavior. This study will take about 10-15 minutes.

What is the purpose of this study?

The purpose of this study is to survey people’s prior experience with secure computing practices and knowledge of information security.

What will I do if I choose to be in this study?

The anonymous, online survey will be administered using a secure website. Once you have read this consent form, and agree to voluntarily participate, you will be taken to a secure website to complete the online survey. You may withdraw from the survey at anytime and you may skip or decline any questions that you do not wish to answer. You will be asked to consider the importance of the data on your device, so this survey should be taken on a personal device.

How long will I be in the study?

Most people take about 10-15 minutes to complete the survey.

What are the possible risks or discomforts?

The risks to you are minimal. They are not greater than those ordinarily encountered in daily life. Please know that this is an anonymous survey that uses a secure link. The survey is anonymous because we will not be able to link your responses back to you we do not ask for any identifiable information (Ex. name). While completing the survey, the only risk to you might be if someone were to see your responses to the survey, so we recommend that you take this survey when you have complete privacy. Since the survey is anonymous, no one will know that you completed this survey unless you personally tell him or her, so breach of confidentiality is a risk and the safeguards used to minimize this risk can be found in the confidential section below.

Are there any potential benefits?

There are no direct benefits to you. Eventually, we hope to publish the research results, and if you want to see them, you should send an email requesting information to the Principal Investigator at XXXXX@purdue.edu.

Will I receive payment or other incentive?

After completing the study, you will be compensated $.40 for your time via the anonymous payment system set up through Mechanical Turk. Participants will not be compensated if they are screened out for the early part of the survey or fail the attention check.

Will information about me and my participation be kept confidential?

We do not ask for your name or any other information that could be used to identify you at any time before, during, or after the survey. No IP addresses will be recorded. There will be no way to determine where the survey was taken or by whom. Instead, the survey software will randomly assign an ID number to your responses. This means that the responses to the questionnaires cannot be linked or matched to you, which means your responses will remain completely anonymous. Only researchers associated with this study will have access to the data. In addition to the data being anonymous, it will be stored electronically in an encrypted format.

The encrypted data will be kept indefinitely and will be used only for research purposes.

The project's research records may be reviewed by the study sponsor/funding agency, Food and Drug Administration (if FDA regulated), US DHHS Office for Human Research Protections, and by departments at Purdue University responsible for regulatory and research oversight.

What are my rights if I take part in this study?

Your participation in this study is voluntary. You may choose not to participate or, if you agree to participate, you can withdraw your participation at any time without penalty or loss of benefits to which you are otherwise entitled.

Who can I contact if I have questions about the study?

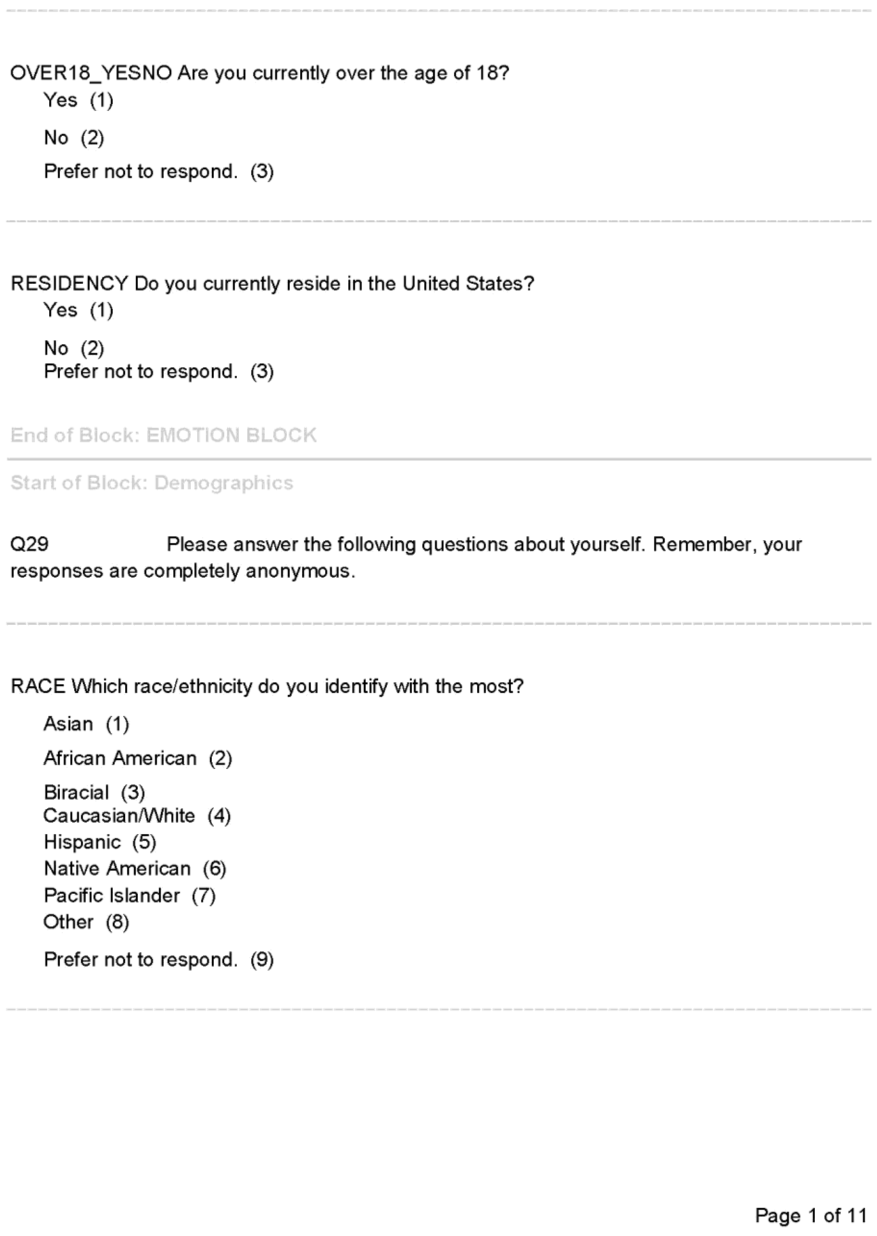
If you have questions, comments or concerns about this research project, you can talk to one of the researchers. Please contact Dr. Kathryn Seigfried-Spellar at XXXXXX. To report anonymously via Purdues Hotline see www.purdue.edu/hotline. If you have questions about your rights while taking part in the study or have concerns about the treatment of research participants, please call the Human Research Protection Program at (765) 494-5942, email (irb@purdue.edu) or write to: Human Research Protection Program - Purdue University Ernest C. Young Hall, Room 1032 155 S. Grant St. West Lafayette, IN 47907-2114

Documentation of Informed Consent

I have had the opportunity to read this consent form and have the research study explained. I have had the opportunity to ask questions about the research study, and my questions have been answered. I am prepared to participate in the research study described above. If I wish, I may print this form for my records. If you agree, please click on the I Agree button below.

Otherwise, we thank you for your time and ask that you click on the I Do Not Agree button.

APPENDIX E. SURVEY



OVER18_YESNO Are you currently over the age of 18?

Yes (1)

No (2)

Prefer not to respond. (3)

RESIDENCY Do you currently reside in the United States?

Yes (1)

No (2)

Prefer not to respond. (3)

End of Block: EMOTION BLOCK

Start of Block: Demographics

Q29 Please answer the following questions about yourself. Remember, your responses are completely anonymous.

RACE Which race/ethnicity do you identify with the most?

Asian (1)

African American (2)

Biracial (3)

Caucasian/White (4)

Hispanic (5)

Native American (6)

Pacific Islander (7)

Other (8)

Prefer not to respond. (9)

Page 1 of 11

SEX What is your sex?

Male (1)

Female (2)

Other (3)

Prefer not to respond. (4)

MARRIAGE_STATUS Which of the following best applies to you (please select one):

Single, never married (1)

Common-Law or Civil Union (2)

Married (3)

Separated (4)

Divorced (5)

Widowed (6)

Prefer not to respond. (7)

EDUCATION Which of the following is your highest level of completed education to date (please select one):

Less than 12 years of high school or secondary education (1)

High School or Secondary Education (2)

Associaties Degree (3)

Bachelors Degree (4)

Masters Degree (5)

PhD/JD/MD (6)

Prefer not to respond. (7)

EMPLOYMENT Which of the following is your current employment status (please select one):

Employed Full-Time (1)

Employed Part-Time (2)

Retired (3)

Student (4)

Unemployed (5)

Prefer not to respond. (6)

INCOME What is your current annual income range from only employment sources (please select one):

$0-$20,000 (1)
$20,001-$40,000 (2)
$40,001-$60,000 (3)
$60,001-$80,000 (4)
$80,001-$100,000 (5)
More than $100,001 (6)

Prefer not to respond. (7)

End of Block: Demographics

Start of Block: MOOD_INDUCTION

SUDOKU_DISPLAY Before the study begins, you must participate in an activity. You must complete a sudoku puzzle.

Sudoku is a game in which there are 81 boxes. Each row (horizontal) and each column (vertical) must contain the numbers 1-9. Each number can only exist once per row and column. There is only one correct solution per puzzle.

You must attempt to solve the puzzle below in 5 minutes. Good luck. This survey will automatically end the game after the time is up.

End of Block: MOOD_INDUCTION

Start of Block: STAI_6

ANXIETY_SCALE A number of statements which people have used to describe themselves are given below. Read each statement and then circle the most appropriate number to the right of the statement to indicate how you feel right now, at this moment.

There are no right or wrong answers. Do not spend too much time on any one statement but give the answer which seems to describe your present feelings best.

	Not at all (1)	Somewhat (2)	Moderately (3)	Very much (4)	I decline to respond. (5)
I feel calm. (1)					
I am tense. (2)					
I feel upset. (3)					

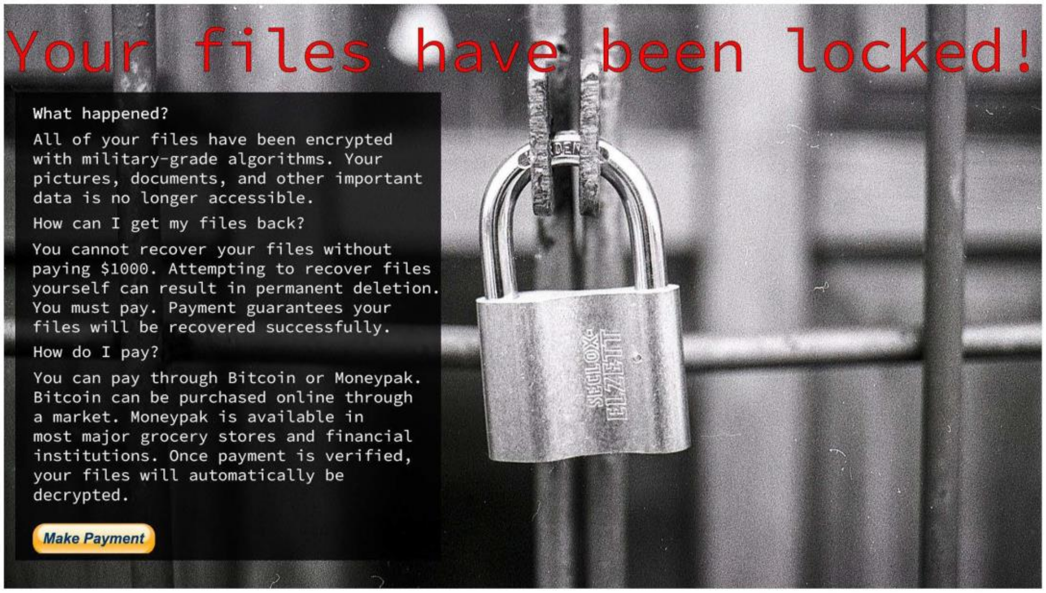
I am relaxed. (4)
I feel content. (5)
I am worried. (6)

End of Block: STAI_6

Start of Block: RANSOMWARE_NORMAL_VIGN

RANSOMWARE_DEFAULT You are at home using your personal computer. You are in the middle of streaming a movie when this image suddenly appears. You cannot exit out of the screen, and all of your files are inaccessible. You attempt to restart your computer, but this screen immediately appears again.

Please consider this situation for at least 60 seconds.



Your files have been locked!

What happened?

All of your files have been encrypted with military-grade algorithms. Your pictures, documents, and other important data is no longer accessible.

How can I get my files back?

You cannot recover your files without paying $1000. Attempting to recover files yourself can result in permanent deletion. You must pay. Payment guarantees your files will be recovered successfully.

How do I pay?

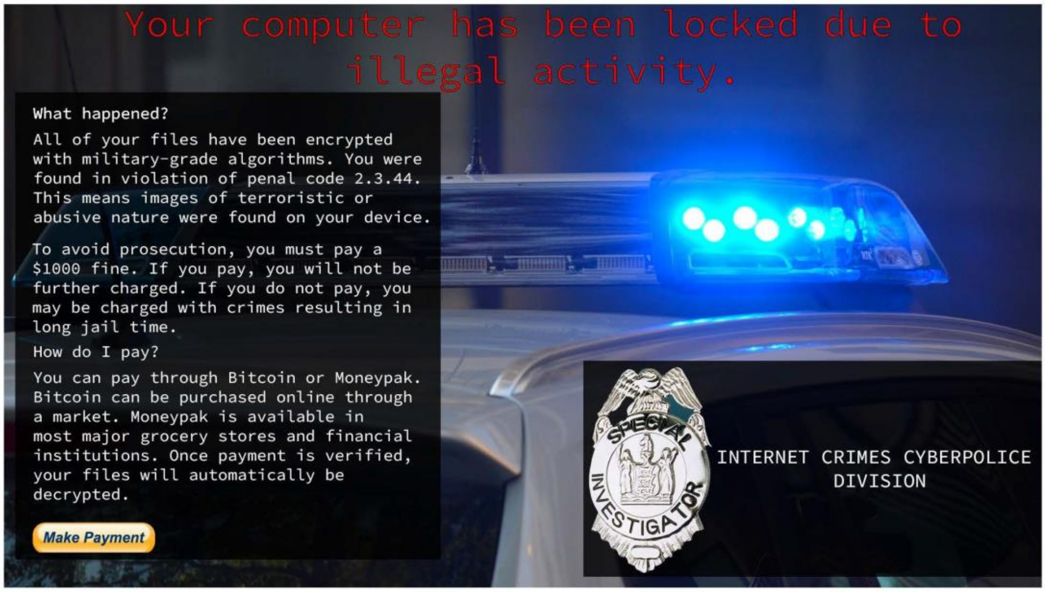
You can pay through Bitcoin or Moneypak. Bitcoin can be purchased online through a market. Moneypak is available in most major grocery stores and financial institutions. Once payment is verified, your files will automatically be decrypted.

End of Block: RANSOMWARE_NORMAL_VIGN

Start of Block: RANSOMWARE_LEO_VIGN

RANSOMWARE_LEO You are at home using your personal computer. You are in the middle of streaming a movie when this image suddenly appears. You cannot exit out of the screen, and all of your files are inaccessible. You attempt to restart your computer, but this screen immediately appears again.

Please consider this situation for at least 60 seconds.



Your computer has been locked due to illegal activity.

What happened?

All of your files have been encrypted with military-grade algorithms. You were found in violation of penal code 2.3.44. This means images of terroristic or abusive nature were found on your device.

To avoid prosecution, you must pay a $1000 fine. If you pay, you will not be further charged. If you do not pay, you may be charged with crimes resulting in long jail time.

How do I pay?

You can pay through Bitcoin or Moneypak. Bitcoin can be purchased online through a market. Moneypak is available in most major grocery stores and financial institutions. Once payment is verified, your files will automatically be decrypted.

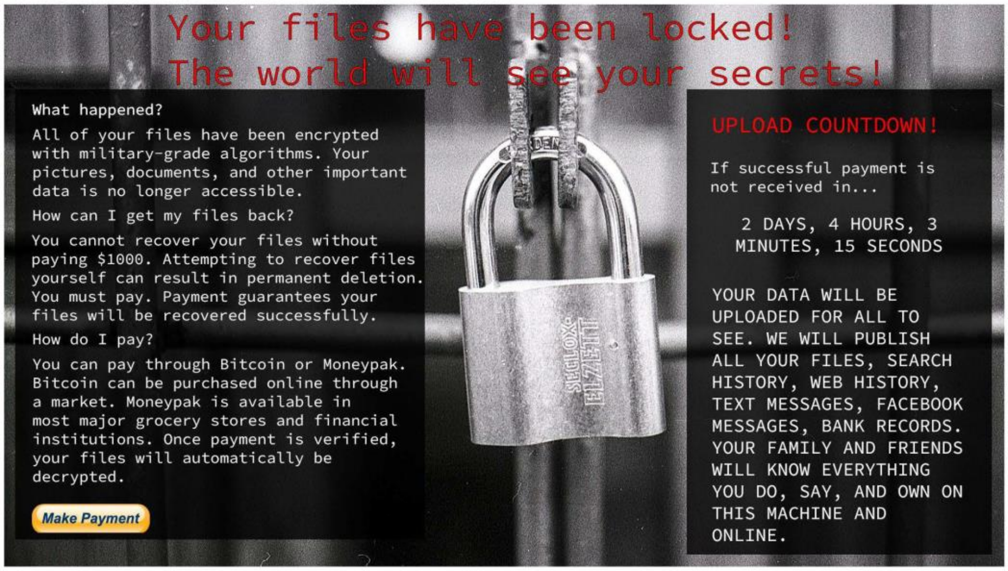
INTERNET CRIMES CYBERPOLICE DIVISION

End of Block: RANSOMWARE_LEO_VIGN

Start of Block: RANSOMWARE_THREAT_VIGN

RANSOMWARE_UPLOAD You are at home using your personal computer. You are in the middle of streaming a movie when this image suddenly appears. You cannot exit out of the screen, and all of your files are inaccessible. You attempt to restart your computer, but this screen immediately appears again.

Please consider this situation for at least 60 seconds.



Your files have been locked!
The world will see your secrets!

What happened?

All of your files have been encrypted with military-grade algorithms. Your pictures, documents, and other important data is no longer accessible.

How can I get my files back?

You cannot recover your files without paying $1000. Attempting to recover files yourself can result in permanent deletion. You must pay. Payment guarantees your files will be recovered successfully.

How do I pay?

You can pay through Bitcoin or Moneypak. Bitcoin can be purchased online through a market. Moneypak is available in most major grocery stores and financial institutions. Once payment is verified, your files will automatically be decrypted.

UPLOAD COUNTDOWN!

If successful payment is not received in...

2 DAYS, 4 HOURS, 3 MINUTES, 15 SECONDS

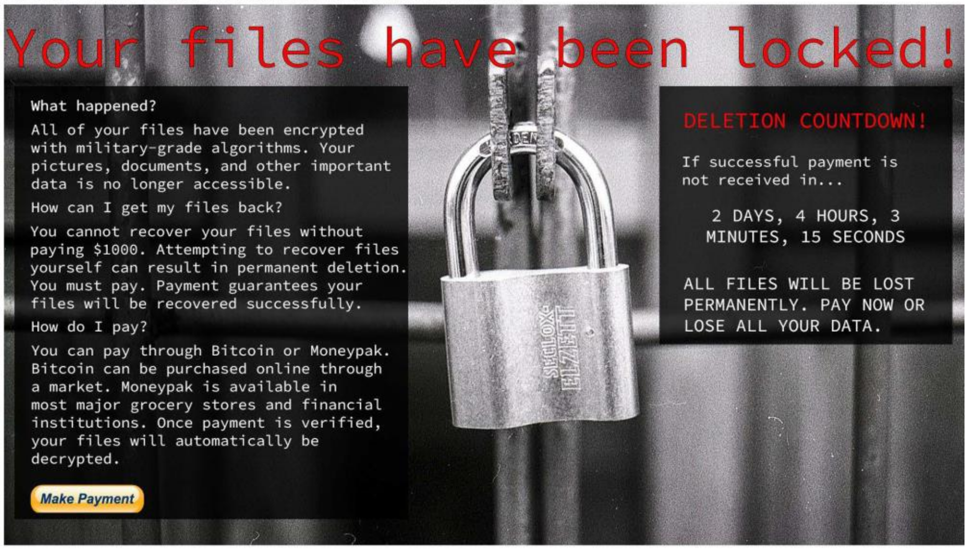
YOUR DATA WILL BE UPLOADED FOR ALL TO SEE. WE WILL PUBLISH ALL YOUR FILES, SEARCH HISTORY, WEB HISTORY, TEXT MESSAGES, FACEBOOK MESSAGES, BANK RECORDS. YOUR FAMILY AND FRIENDS WILL KNOW EVERYTHING YOU DO, SAY, AND OWN ON THIS MACHINE AND ONLINE.

End of Block: RANSOMWARE_THREAT_VIGN

Start of Block: RANSOMWARE_TIMER_VIGN

RANSOMWARE_COUNTDOWN You are at home using your personal computer. You are in the middle of streaming a movie when this image suddenly appears. You cannot exit out of the screen, and all of your files are inaccessible. You attempt to restart your computer, but this screen immediately appears again.

Please consider this situation for at least 60 seconds.



Your files have been locked!

What happened?

All of your files have been encrypted with military-grade algorithms. Your pictures, documents, and other important data is no longer accessible.

How can I get my files back?

You cannot recover your files without paying $1000. Attempting to recover files yourself can result in permanent deletion. You must pay. Payment guarantees your files will be recovered successfully.

How do I pay?

You can pay through Bitcoin or Moneypak. Bitcoin can be purchased online through a market. Moneypak is available in most major grocery stores and financial institutions. Once payment is verified, your files will automatically be decrypted.

Make Payment

DELETION COUNTDOWN!

If successful payment is not received in...

2 DAYS, 4 HOURS, 3 MINUTES, 15 SECONDS

ALL FILES WILL BE LOST PERMANENTLY. PAY NOW OR LOSE ALL YOUR DATA.

End of Block: RANSOMWARE_TIMER_VIGN

Start of Block: POST_RANSOMWARE

RANSOMWARE_RESPONSE The previous screen simulated a **real** ransomware infection scenario. Ransomware is a type of virus which takes your files and demands payment in exchange for returning them. Please answer the following questions **as you felt** when you saw the screen.

Please answer how you would have actually responded if this attack had happened to your device.

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)	I decline to respond. (6)
I would have paid the ransom. (1)						
I would not have given money to the attacker. (2)						
I was afraid of losing my files. (3)						

RANSOMWARE_NOYES If you had to choose, would you have paid the ransom?

No (1)

Yes (2)

RANSOMWARE_WHYPAY Why did you choose to pay the ransom?

____

____

RANSOMWARE_WHYNOTPAY Why did you choose not to pay the ransom?

____

____

ALTERNATIVES You stated you would not pay the ransom. The following statements also describe how someone may respond to a ransomware attack. Please indicate how likely you would be to take the following actions.

	Very unlikely (1)	Unlikely (2)	Neither likely nor unlikely (3)	Likely (4)	Very likely (5)	I decline to respond. (6)
I would have contacted law enforcement. (1)						
I would have asked a more computer-knowledgeable individual for help (such as a friend or family member). (2)						
I would have called my computer's technical support line (such as Dell or 1-800-MY-APPLE). (3)						
I would have taken my computer to an IT help desk (such as the Geek Squad at Best Buy). (4)						
I would do nothing, because I already have my data backed up. (5)						

PAYSCALES Ransom prices vary; therefore, we would be interested in which ransom price range you would pay. Please **select all options** in which you would have paid the ransom in that price range.

$1-100 (1)

$101-200 (2)

$201-300 (3)

$301-400 (4)

$401-500 (5)

$501-600 (6)

$601-700 (7)

$801-900 (8)

$901-1000 (9)

I would have paid over $1000. (10)

I would not have paid the ransom at any price. (11)

I decline to respond. (12)

End of Block: POST_RANSOMWARE

Start of Block: INFOSEC_QUESTIONS

INFOSEC_BLK1 Please answer the following questions to the best of your ability.

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)	I decline to respond. (6)

I had formal training on common computer security practices. (1)
I read computer security-related newsletters or articles before. (2)
I use different passwords for different accounts. (3)
The organization I worked for had an established information security policy. (4)
The organization I worked for has provided employees with information security training. (5)
The organization I worked for has provided employees with security-related newsletters or articles. (6)

INFOSEC_BLK2 Please answer the following questions to the best of your ability.

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)	I decline to respond. (6)
My colleagues at work update their computers regularly. (1)						
I believe other employees in my organization back up their computers regularly. (2)						
I am convinced that other employees comply with the organization's information security policy (if the organization has one). (3)						
The majority of employees in my organization attend cyber security training. (4)						

INFOSEC_BLK2 Please answer the following questions to the best of your ability.

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)	I decline to respond. (6)
My organization constantly reminds me to practice its computer and Internet security policies. (1)						
I know how to apply security patches to operating systems. (2)						
I feel confident in setting the Web browser to different security levels. (3)						
I feel confident in handling virus-infected files. (4)						
I feel confident in getting rid of spyware and malware from my computer. (5)						
I have the skills to implement security measures to stop people from getting my confidential information. (6)						
I have the skills to implement security measures to stop people from damaging my computer. (7)						

ATTENTION_CHECK Please answer the following questions to the best of your ability. To ensure you are paying attention, please select "Strongly disagree" regardless of your true feelings.

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
I feel happy right now. (1)					

INFOSEC_BLK3 Please answer the following questions to the best of your ability.

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)	I decline to respond. (6)

I use different passwords for my different social media accounts. (1)
I usually review privacy/security settings on my social media sites. (2)
I keep the anti-virus software on my computer up to date. (3)
I watch for unusual computer behaviors/responses (e.g., computer slowing down or freezing up, pop-up windows, etc.) (4)
I do not open email attachments from people whom I do not know. (5)
I have never sent sensitive information (such as account numbers, passwords, and social security numbers) via email or using social media. (6)
I back up important files on my computer. (7)
I always act on any malware alerts that I receive. (8)
I don't click on short URLs posted on social media sites unless I know where the links will really take me. (9)

End of Block: INFOSEC_QUESTIONS

LIST OF REFERENCES

Alhazmi, O. H., & Malaiya, Y. K. (2013). Evaluating Disaster Recovery Plans Using the Cloud. In *2013 proceedings annual reliability and maintainability symposium (rams)* (pp. 1–6).

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: a Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS quarterly*, *34*(3), 613–643.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender Difference and Employees' Cybersecurity Behaviors. *Computers in Human Behavior*, *69*, 437–443.

Apel, M., Bockermann, C., & Meier, M. (2009). Measuring Similarity of Malware Behavior. In *Local computer networks, 2009. lcn 2009. ieee 34th conference on* (pp. 891–898).

Arditte, K. A., Çek, D., Shaw, A. M., & Timpano, K. R. (2016). The Importance of Assessing Clinical Phenomena in Mechanical Turk Research. *Psychological Assessment*, *28*(6), 684.

AV-Comparitives. (2019). *IT Security Survey 2019*. Retrieved from https://www.av-comparatives.org

Aytes, K., & Conolly, T. (2003). A Research Model for Investigating Human Behavior Related to Computer Security. *AMCIS 2003 Proceedings*, 260.

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to Better how to Make Bitcoin a Better Currency. In *International conference on financial cryptography and data security* (pp. 399–414).

Bayoumy, Y. (2018). *Cybercrime Economy-a Netnographic Study on the Dark Net Ecosystem for Ransomware*. Unpublished master's thesis, NTNU.

Behrend, T. S., Sharek, D. J., Meade, A. W., & Wiebe, E. N. (2011). The Viability of Crowdsourcing for Survey Research. *Behavior research methods*, *43*(3), 800.

Bossler, A., Holt, T. J., & Seigfried-Spellar, K. C. (2017). *Cybercrime and Digital Forensics: An Introduction*. Routledge.

Brewer, R. (2016). Ransomware Attacks: Detection, Prevention and Cure. *Network Security*, *2016*(9), 5–9.

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

Caulfield, T., Ioannidis, C., & Pym, D. (n.d.). Dynamic Pricing for Ransomware.

Chen, Q., & Bridges, R. A. (2017). Automated Behavioral Analysis of Malware a Case Study of WannaCry Ransomware. *arXiv preprint arXiv:1709.08753*.

Constantin, L. (2016, Apr). *Jigsaw Crypto-Ransomware Deletes More Files the Longer you Delay Paying.* CSO. Retrieved from https://www.csoonline.com/

Corrigan, K. (2017). *Ransomware: A Growing Epidemic For Business*. Unpublished doctoral dissertation, Utica College.

Couper, M. P., Kapteyn, A., Schonlau, M., & Winter, J. (2007). Noncoverage and Nonresponse in an Internet Survey. *Social Science Research*, *36*(1), 131–148.

Field, A. (2009). *Discovering Statistics Using SPSS*. Sage publications.

Fleischer, A., Mead, A. D., & Huang, J. (2015). Inattentive Responding in Mturk and Other Online Samples. *Industrial and Organizational Psychology*, *8*(2), 196–202.

Goodman, J. K., Cryder, C. E., & Cheema, A. (2013). Data Collection in a Flat World: The Strengths and Weaknesses of Mechanical Turk Samples. *Journal of Behavioral Decision Making*, *26*(3), 213–224.

Hampton, N., & Baig, Z. A. (2015). Ransomware: Emergence of the Cyber-Extortion Menace.

Hernandez-Castro, J., Cartwright, E., & Stepanova, A. (2017). Economic Analysis of Ransomware.

Hyman, P. (2013). Cybercrime: It’s Serious, but Exactly How Serious? *Communications of the ACM*, *56*(3), 18–20.

IBM. (n.d.). *IBM SPSS GLM Options.* Retrieved from https://www.ibm.com/

Isen, A. M., & Gorgoglione, J. M. (1983). Some Specific Effects of Four Affect-

Induction Procedures. *Personality and Social Psychology Bulletin*, *9*(1), 136–143.

Jung, N., Wranke, C., Hamburger, K., & Knauff, M. (2014). How Emotions Affect Logical Reasoning: Evidence From Experiments With Mood-Manipulated Participants, Spider Phobics, and People With Exam Anxiety. *Frontiers in psychology*, *5*, 570.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting The Gordian Knot: a Look Under The Hood Of Ransomware Attacks. In *International conference on detection of intrusions and malware, and vulnerability assessment* (pp. 3–24).

Korolov, M. (2017, May). *Report: Average Ransomware Demand Now Over $1,000.* CSO. Retrieved from https://www.csoonline.com/

Lab, K. (2016, Sep). *The Cost of Cryptomalware: Smbs at Gunpoint.* Retrieved from https://www.kaspersky.com/

Landis, J. R., & Koch, G. G. (1977). The Measurement of Observer Agreement for Categorical data. *biometrics*, 159–174.

Liao, K., Zhao, Z., Doupé, A., & Ahn, G.-J. (2016). Behind Closed Doors: Measurement and Analysis of Cryptolocker Ransoms in Bitcoin. In *Electronic crime research (ecrime), 2016 apwg symposium on* (pp. 1–13).

Luo, X., & Liao, Q. (2007). Awareness Education as the Key to Ransomware Prevention.

Information Systems Security, *16*(4), 195–202.

Malwarebytes. (2016, Aug). *Inside Chimera Ransomware - the First 'doxingware' in Wild. Malwarebytes*. Retrieved from https://blog.malwarebytes.com/

Mansfield-Devine, S. (2016). Ransomware: Taking Businesses Hostage. *Network Security, 2016*(10), 8–17.

Marquis, K. H., Marquis, M. S., & Polich, J. M. (1986). Response Bias and Reliability in Sensitive Topic Surveys. *Journal of the American Statistical Association, 81*(394), 381–389.

Marteau, T. M., & Bekker, H. (1992). The Development of a Six-Item Short-Form of the State Scale of the Spielberger Statetrait Anxiety Inventory (STAI). *British Journal of Clinical Psychology, 31*(3), 301–306.

Martins, A., & Elofe, J. (2002). Information Security Culture. In *Security in the information society* (pp. 203–214). Springer.

Milošević, N. (2013). History of Malware. *arXiv preprint arXiv:1302.5392*.

Morgan, S. (2016). *Cybercrime Damages Expected to Cost the World $6 Trillion by 2021.*

CSO. O'Gorman, G., & McDonald, G. (2012). *Ransomware: A Growing Menace*. Symantec Corporation.

Pacheco-Unguetti, A. P., Acosta, A., Callejas, A., & Lupiáñez, J. (2010). Attention and Anxiety: Different Attentional Functioning Under State and Trait Anxiety. *Psychological science, 21*(2), 298–304.

Pope, J. (2016). Ransomware: Minimizing the Risks. *Innovations in clinical neuroscience*, *13*(11-12), 37.

Richardson, R., & North, M. (2017). Ransomware: Evolution, Mitigation and Prevention. *International Management Review*, *13*(1), 10–21.

Salazar, M. S. (2015). The Dilemma of Combining Positive and Negative Items in Scales. *Psicothema*, *27*(2), 192–200.

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016). Cryptolock (and Drop it): Stopping Ransomware Attacks on User Data. In *Distributed computing systems (icdcs), 2016 ieee 36th international conference on* (pp. 303–312).

Segura, J. (2016, Mar). FBI *Ransomware now targeting Apple's Mac OS X Users.*
Malwarebytes.
Retrieved from https://blog.malwarebytes.com/

Shannon, D. M., Johnson, T. E., Searcy, S., Lott, A., et al. (2002). Using Electronic Surveys: Advice from Survey Professionals. *Practical assessment, research & evaluation*, *8*(1), 1–2.

Sittig, D. F., & Singh, H. (2016). A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. *Applied clinical informatics*, *7*(2), 624.

Westermann, R., Spies, K., Stahl, G., & Hesse, F. W. (1996). Relative Effectiveness and Validity of Mood Induction Procedures: A meta-analysis. *European Journal of social psychology*, *26*(4), 557–580.

White, G. L. (2015). Education and Prevention Relationships on Security Incidents for Home Computers. *Journal of Computer Information Systems*, *55*(3), 29–37.

Work, H. D. M. (2011). IO and the Crowd: Frequently Asked Questions About Using Mechanical Turk for Research. *TIP*, 11.

Zolkipli, M. F., & Jantan, A. (2010). Malware Behavior Analysis: Learning and Understanding Current Malware Threats. In *Network applications protocols and services (netapps), 2010 second international conference on* (pp. 218–221).