12-2020

In-Depth Analysis of College Students' Data Privacy Awareness

Vernon D. Andrews

Follow this and additional works at: https://csuepress.columbusstate.edu/theses_dissertations

Part of the Computer Sciences Commons

Recommended Citation

www.manaraa.com

COLUMBUS STATE UNIVERSITY

IN-DEPTH ANALYSIS OF COLLEGE STUDENTS' DATA PRIVACY AWARENESS

A THESIS SUBMITTED TO

THE TURNER COLLEGE OF BUSINESS

IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF CYBERSECURITY MANAGEMENT

TSYS SCHOOL OF COMPUTER SCIENCE

BY

VERNON D. ANDREWS

COLUMBUS, GEORGIA

2020

IN-DEPTH ANALYSIS OF COLLEGE STUDENTS' DATA PRIVACY AWARENESS

By

Vernon D. Andrews

Committee Chair:
Dr. Lydia Ray

Committee Members

Dr. Radhouane Chouchane
Dr. Lixin Wang

Columbus State University

December 2020

ABSTRACT:

While attending university, college students need to be aware of issues related to data privacy. Regardless of the age, gender, race, or education level of college students, every student can relate to the advancement of the internet within the last decades. The internet has completely transformed the way the world receives and stores messages. Positively, the internet allows messages to be sent across the globe within the fraction of a second and provides students with access to potentially unlimited information on a variety of subjects. On the downside, there are issues on the internet that can cause more harm than good. Most college students automatically think the internet is secure; however, the internet is full of loopholes that allow hackers to expose them on the internet and utilize them to exploit individuals for monetary gains. Within the last decade, there has been an enormous number of data breaches that have pinpointed the lack of awareness regarding data privacy. Do college students, who utilize the Internet for entertainment and education, know about the issue of data privacy on the Internet? In this thesis, I have proposed a modern method that carefully analyzes the data privacy level amongst college students. To ensure ultimate data privacy, we must initially create the awareness then analyze the awareness of data privacy. To adequately address the fundamental issues of data privacy, students will be respectfully asked to satisfactorily complete a structured questionnaire. The questionnaire will measure students' competence level regarding data privacy. The observational data will be utilized to uniquely determine if students are aware of the issues of data privacy or not. After further analysis, the data will be used to determine if there are unique characteristics that separates those who are aware from those who are not aware. The characteristics will be age, education, race, and exposure to computer related classes.

INDEX WORDS: Data Privacy, Data Awareness, Data Privacy Competence, Encryption, Cryptography

ACKNOWLEDGMENTS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

IN-DEPTH ANALYSIS OF COLLEGE STUDENTS' DATA PRIVACY AWARENESS

A thesis submitted to Turner School of Business

in partial fulfillment of the requirements for the degree of

MASTER OF CYBERSECURITY MANAGEMENT

TSYS OF COMPUTER SCIENCE

By

Vernon D. Andrews

2020

Lydia Ray
_____

Dr. Lydia Ray, Chair

2/16/2021
_____

Date

Radwan Shushane
_____

Dr. Radhouane Chouchane, Member

4/15/2021
_____

Date

Lixin Wang
_____

Dr. Lixin Wang, Member

4/15/2021
_____

Date

1.   INTRODUCTION

1.1   Cyber Attacks

Within the last decade, the number of cyberattacks has increased dramatically. According to researchers from the Pew Research Center, cyberattacks will continue to increase at an exponential rate within the next few years (Rainie, Anderson, & Connolly, 2020). Some of the attacks that instantly became notable in the world are listed in the Table 1 (Notable Cyber Attacks) below:

Table 1(Notable Cyber Attacks):

Name of Company	Company's Information	Hacking Date	# of users account exposed
Abode	Computer software	October 2013	153 million
Adult Friend Finder	Dating Service	October 2016	412.2 million
Canva	Graphic design	May 2019	137 million
Dubsmash	Video messaging service	December 2018	162 million
eBay	Online auction	May 2014	145 million
Equifax	Credit bureau	July 2017	147.9 million
Heartland Payment Systems	Card transaction	March 2008	134 million
LinkedIn	Social network	June 2012 & May 2016	165 million
Marriott Int.	Hotel	2014-18	500 million

My Fitness Pal	Fitness app	February 2018	150 million
Myspace	Social Media	June 2013	360 million
NetEase	Mailbox services	October 2015	235 million
Sina Weibo	Social Media	March 2020	538 million
Yahoo	Web services	2013-14	3 billion
Zynga	Gaming	September 2019	218 million

Not only did the attacks become notable but they also exposed the hundreds of vulnerabilities in the cybersecurity infrastructure of these organizations (Swinhoe, 2020). One of the major known vulnerabilities that always becomes exploited is human error. Human error, in cybersecurity context, is defined as unintentional actions - or lack of action - by employees and users that cause, spread or allow a security breach to take place (Aloha, 2020). Among all attacks that exploit human error and human vulnerability, social engineering is the most common and most frequent. And among all social engineering attacks, phishing emails are the most popular because these are easy to launch, and chances of successful attack are high. Now that we are in the middle of the coronavirus pandemic, cyberattack experts have seen a 600 percent spike in malicious emails (Miller, 2020). One significant harm caused by cyberattacks and data breaches is that they can expose and collect people's private information. Most individuals might not agree with promoting data privacy awareness but there are at least two reasons why promoting data privacy awareness is important. One is that data breaches can expose a lot of private data. In 2016, Adult Friend Finder was hacked and exposed to over 412 millions of their users' private lives which resulted in some suicides. The other reason is that attackers can use private information for constructing sophisticated spear-phishing emails. Phishing emails can manipulate users onto a fake domain site

that can monitor their users' logins and passwords. For example, a phishing email can be strategically designed for a particular person that seems legit but in reality, is an attempt made to lure that person into entering their user's login information.

Checking emails is a task that many college students perform daily. With checking emails, students have to become aware of the enticing tools that hackers use to get students to perform human errors when checking for soliciting emails such as coupon codes, honor committee, flash sales, etc. The importance of becoming aware of data privacy is extremely high. Most college students don't seem to think checking and clicking emails can expose them to becoming a potential victim or comprising their computer network. The approach here is to analyze whether college students are or are not aware of the issues related to data privacy. After researching this topic, it is safe to say that there is no such article that analyzes data privacy amongst college students.

1.2   Data Privacy

What is data privacy, and how do we measure data privacy? As technology evolves, we clearly realize more and more issues related to data privacy. Data privacy has officially become an essential tool that all or almost every college student needs to explore the internet. One of the main issues related to data privacy is the awareness of data privacy. Most college students are not aware of the issues related to data privacy. So, how do we explore these issues? Well, a person can start by educating themselves by going to school and pursuing a degree in the computer science realm. Another way is particularly, trial and error. The ways of trial and error is the worst approach, in my opinion, but can be necessary in today's world. But how do we reach those who are not pursuing a degree in computer science and those who are less fortunate to not have Internet access on a daily basis as it pertains to the majority of the world?

As the Internet and technology evolves, we continue to transform into a digital world. According to studies, the digital world is one of the most transformational systems that this world has ever seen, and we have completely gone 'digital' (Warman, 2020). We have transformed from sending messages across the world in paper bottles on boats to sending messages across the world within a fraction of a second, digitally. With all the new advancements in technology and current updates on the internet, there have posed a lot of security risks.

1.3   Risks Associated with Data Privacy

There are security risks that focus on individuals' aspects that can expose a person's information on the internet. These risks can also be potentially used against them for probable gains. This is the loophole that technology experts avoided sharing at first. Almost every person in this world can relate to some type of advancement in technology. For example, the average car is compacted with Bluetooth, on-star equipment, digital dashboard ups, etc. The average household has two or more computers running at all times. The average school has online programs where students can complete their courses as needed to obtain their degree. In the digital commerce world, a person can go into a grocery store and purchase any item with just the tap of a bank card. With the advancement of technology, there are a lot of issues pertaining to security risks. Particularly towards college students, they can be at an advantage and a disadvantage in how they conduct their daily activities on the internet.

1.4   Data Privacy Concerns for College Students

Most college students conduct their daily activities for a particular course as given by an instructor, without being aware of the security risk related to the internet. They assume that surfing

the web from an incognito window or a non-incognito window produces the same ramifications. Well, in an incognito window, any information that is inputted into the windows is not traceable. This window particularly works great for any information such as your id number, debit card information, personal address, phone number, and any type of personal information that can potentially expose a person's identity. Even though some college students tend to be nonchalant about the fact that hackers can steal their identity; it is a known fact that the majority of college students love to respond to solicit emails from unknown addresses. In this study, a question states: John Doe receives an email from Geg.com, which is basically known for soliciting information from individuals and stealing their information in hopes of exposing new victims. So, John receives an email from Geg.com and the email states that "you have been highly selected to win a trip to the Bahamas for three or more people, now that you have my selected all we need is your information for you to secure your win by adding by creating an account and adding a debit card with a one-dollar charge on file so that your win number can be secured". Well, some students think that John just got lucky because there are credible companies that have given away numerous products to college students such as Apple and Amazon. There is a distinguished connection between Geg.com and Apple, but a person with a low competence data level cannot make the connection.

1.5   Social Engineering (Phishing Attack)

A company of high value, such as Apple, in this instance will not diminish their reputation by soliciting college students to obtain their information and steal their customers' data by manipulating students into putting in personal information. However, Geg.com is exquisitely known for this type of strategy. This is a problem that this thesis would like to address. Most college students are not aware of the basic social engineer tactics that hackers use on the Internet. Social engineering such as phishing attacks is a tactic that hackers use to solicit personal and valuable

information from a particular person, or multiple people of interest. Interestingly, what's exciting about phishing attacks is the engineering behind each attack. It can convince a person that the false information is real, authentic, and secure. For example, the average college student might go to their local Starbucks to access the local Starbucks' WIFI to complete an assignment. However, a student might not know a hacker who is possibly sitting in that same coffee shop can create a fake domain with the same name as Starbucks. If the students connect to the fake domain, the hacker can then use any information that the student inputs and monitor their login information to steal their personal identity.

Students should be able to recognize the difference in a domain name. It's more than just staying away from insecure sites. Staying off insecure sites can be helpful but it's best to have an overall view on how to protect your personal information. In the Starbucks case, a fake domain Starbucks WIFI is only used as a trap holder that steals anyone who is connected to it. This theoretical example is a type of real-life scenario that can happen to any college student in the world. If students are not aware of these tactics, it can specifically ruin them financially. Not only can it ruin them, but it can also ruin their college infrastructure depending if they are logged onto their school's website. Hackers love to use this type of fake domain name approach, as a safe way to protect their identity. It's ironic that hackers love to protect their identities; so, shouldn't we do the same? Connecting to a fake domain is only the tipping point of the iceberg that hackers use in a data breach. However, I believe that all college students should have knowledge of the basic steps on how to protect their personal information. In this research, college students will be surveyed and analyzed to determine whether they are aware of the issues related to data privacy or not.

1.6   Cyber Attacks' Weakest link

It's not the average student's fault that they are not aware of the tactics that hackers use, it's a new topic that has recently been exposed. As reported, cyber-attacks are increasingly rising every

single day (Symanovich, 2020). As we move forward in his world, we will notice more cyber-attacks that will occur. A vast amount of research has identified the main cause of cyber-attacks. Cyber-attacks occur because of human errors. Human errors are defined as unintentional actions or lack of action by employees and users that cause, spread, or allow a security breach to take place (Ahola, 2020). As continuing from the Starbucks example, a college student logged onto a fake Starbucks domain can connect without realizing the fake domain name's StarbucksX. Rushing to submit an assignment, led the student to input their credentials into StarbucksX and potentially used against them in the long run.

Furthermore, we could also discuss the different tactics that hackers use in addition to creating fake domains to entice individuals by creating fake strong bandwidth connections, colors that are familiar with their targeted company, etc. But in this case, we want to study how college students review their privacy.

In this thesis, students will be tested on their basic level of awareness l. The main goal of this thesis is to explore whether college students are aware of issues of data privacy or not aware. If the study proves that students are not aware of the data privacy issues, a solution will be proposed in an attempt to better educate college students on this issue.

2. LITERATURE REVIEW

Why measure data privacy competence? A person that acquires a high data awareness level categorizes them as a low risk breached victim. Likewise, a person with a low data awareness level categorizes them as a high-risk potential breach victim (Andrews, 2019). A low-risk person is someone less likely to become victimized in a breach and a high-risk person can more than likely become a victim. Individuals must understand the risk factors involved in a data breach. So again, why measure someone's data awareness level? Data breaches and cyber-attacks will only increase

in the future (Rainie, Anderson, & Connolly, 2019). There is a lot of valuable information that can be stolen or compromised in a data breach. With regard to a company or organization, their data can be stolen and sold on the Dark web for potential gain. On a personal level, private information such as social security numbers, addresses, phone numbers, email addresses, etc., can be stolen and used to conceal a person's identity. Their area of research is quite vague, and a few studies have been made to analyze the problem. Researchers from Germany conducted a data analysis study on German middle school students. The study concluded that most students did not have a data competence mentality (Hug, 2018). Their approach to measuring middle school students was very unique. But as research shows, the only way cyber-attacks and data breaches can decline is if a person becomes aware of the issues. If students are not aware of the data privacy issues, then hopefully educating them will curb the numerous attacks that are projected to occur in the future. Promoting data awareness and educating students is extremely necessary.

This research project engages in several areas of research that relate to cybersecurity, data protection, cyber awareness, and data competence awareness. There are many researchers that have attempted to explore these areas. Measuring data privacy amongst college students can produce valuable material and provide some valuable information.

Some students that are not in computer science-related studies are misinformed of the potential threats in the cyber realm. Being aware of security issues is a must for students who are not computer science based. A great security awareness provides students with vital and knowledgeable skills in handling real-world security threats and issues. Some areas that an effective security assessment can be utilized with helping students become aware of cyber issues are: "research, troubleshooting, configuration, analysis, and other technical skills" (Kercher & Rowe, 2012). Researchers Kercher and Rowe, from Brigham Young University, wanted to address this problem by implementing an IT cyber training workforce in their university (Kercher & Rowe,

2012). Their workforce consisted of two teams: the blue team and the red team. The red team performed penetration tests and the blue team performed lower-risk tasks such as server hardening and forensic activities. In correlation to analyzing the data privacy level amongst college students, educating students and providing them with hands-on-experience is a great way to start.

The importance of becoming aware of data privacy is becoming one of the greatest concerns to any organization's management. In an organization, there are employees, or insiders, who use their information systems to perform their day-to-day operations tasks. Similar to employees, students are insiders who use their school's information systems for study purposes. An information system is not a surplus anymore in regards for securing data. The only time an information system is valuable is when it is used to compete for market value with their rival companies. However, there are still some things that an organization must do in order to make sure their information system is protected. It takes more than creating and implementing solutions such as firewalls, intrusion detection systems, anti-viruses, etc. Organizations also need to invest in the human factor. The human factor are the employees or students that use their information systems and technology resources.

As technology evolves, the continuous next entrant of the Internet of things (IoT) continues to be the smartwatch. The smartwatch makes it more convenient for a consumer, but no one seems to be educated on the security aspect of the smartwatch. Researchers from the School of Informatics and Computing at Indiana University wanted to explore how college students viewed privacy-awareness, their attitude toward privacy, and how their level and attitude of privacy awareness affect their "smartwatch related privacy-enhancing behavior" (Udoh & Alkharashi, 2016). Smartwatches have been known to perform necessity actions that make it easier on the consumer such as measuring heart rates, counting steps, monitoring sleep, and monitoring general health. However, with these new functions now involving a smartwatch which differs from a 1982 Casio

Seiko calculator watch can put a consumer at risk. regarding privacy. "Privacy violations can portend a whole range of harm, including the sharing of the personal data of a user with a third-party such as health insurance companies for business purposes" (Udoh & Alkharashi, 2016). Researchers wanted to know how college students viewed privacy concerns and privacy violations in regard to the use of smartwatches. Surprisingly, researchers found that students were frightened to think about the security issues of using a smartwatch and they decided not to worry about it on everyday bias. Researchers concluded that some students showed an "I don't care" attitude toward privacy concerns.

In the past, I have researched a similar topic to this issue. My latest research entitled "Analyzing Awareness on Data Privacy" analyzed the awareness level of participants from a wide range of audiences. The audience ranged from ages:18 to 64 who were students, educators, citizens, etc. Each participant was asked to complete a survey (Appendix A). The survey consisted of friendly based questions that put subjects in a position that reflected their everyday life without creating a hassle that reminded the subjects they were taking a survey (Andrews, 2019). The majority of the questions were designed, in particular, to create a fun experience but also seek the importance of raising awareness on issues of data privacy (Andrews, 2019). The results from the study showed that some subjects were not aware of the issues related to data privacy (Andrews, 2019). This research showed that the lack of data privacy awareness was alarming. One subject, even, expressed how some of the questions were similar to the annual questions that their company sends out to their employees every year. The subject further stated that it is critical for every employee to answer every question correctly to the best of their ability or face termination.

3.   RESEARCH STUDY

3.1   Goals

The main research goal of this project is to find out if college students are aware of data privacy issues. To perform this task, the project seeks to survey college students to analyze if they are aware of the issues or not. The survey's questions can be found in Appendix B. Additionally, I hope to find some distinguishing factors that separates college students who are aware from those who are not aware. The factors that will be studied in this thesis are education levels, age, race, and gender. If the study proves that students are not aware then a policy will be created and suggested to be implemented to improve the awareness level of data privacy amongst college students.

3.2   Motivation

Before I became a graduate student at Columbus State University, I noticed the rampage of cyberattacks that were occurring in the world. I realized that I did not want to become a victim in the data world, so I directed my education towards cybersecurity. In the first session of the program, I realized that I did not know anything about cybersecurity. Suddenly, I realized that this lack of knowledge is part of the reason why many cyberattacks occur. Later in the program, I was given the freedom to write a paper on any topic I wanted as long as it was related to computer science. I was in the second half of completing my Cybersecurity Management program, and I began to do a lot of research and noticed there were not any resources or articles in the Galileo database that pertains to studies that analyzed the lack of data privacy amongst college students. Having a background in political science, I wondered how I could reach out to students that had a similar background. I began to research ways to create better passwords, but unfortunately, most articles used computer terms which are difficult for individual outsides of the computer science field to comprehend. Then, I began to study topics such as protecting data on the internet and ways to increase my cyber

education, what steps do I need to take in order to become more aware of cyber issues today, what should I expect next in the cyber world, and where do I start? Most students today do not understand the basics of data privacy. So, I develop a method to help understand whether college students are aware of data privacy and what factors influence their knowledge.

This method was inspired by my recent study that I used to test subjects on their data privacy levels. In that method, I created a questionnaire that tested subjects on their data competence knowledge in the internet realm. As stated earlier, the questions were friendly based and designed to analyze data awareness among participants who took the questionnaire. The questionnaire was divided into three parts: data privacy, the control of someone's data, and encryption. There was a total of 11 questions in the questionnaire. This questionnaire is located in Appendix A. In addition, I wanted to survey only college students and use the same method to test college student's data awareness level but with a deeper approach. In Appendix B, locates the new questionnaire will be used to test college students on their data privacy issues.

3.3 Methodology

As stated, the research purpose of this study is to analyze whether college students were aware of the issues related to data privacy or not. Also, create an in-depth analysis of the distinguishing factors that make certain students aware of data privacy issues than those who are not. The distinguishing factors will be race, education level, age, etc. In order to fulfill this goal, a survey was designed as the main tool to carry out the analysis of this study. The survey is divided into four parts and each part respectively will be used as a measuring tool to analyze whether students have a data privacy competence level or not.

3.4   Research Questionnaire

As stated, the questionnaire is divided into four parts: data privacy, cryptography, control someone's data on the internet, and the participant's information. The questionnaire will test students on their strengths and weaknesses on data privacy.

The first section, data privacy consists of four questions. The questions are designed to analyze college students' awareness level on the issues related to data privacy issues. The questions will measure their awareness level on avoiding scam text messages, avoiding solicit emails, avoiding scam emails, avoiding scam calls, and recognizing real domain names. This section provides an overall view on students' perspective on real-life situations. The students' answer will detect whether students would be deceived by the tricks that the hackers use.

The second section, cryptography, consists of three questions. This section is designed to measure students' cryptography skills. Students must be able to present some type of awareness related to cryptography. Analyzing cryptography can present many challenges and this is by the far the most difficult analysis of this study. Cryptography plays an important role in data privacy. Having a high level of cryptography skills puts a person in a low-risk status of being a victim of cybercrimes. The questions in this section measures student's ability to decipher messages, list the different types of encryption, and define the term cryptography. Hence note, encryption methods are the best way to create a strong password and are highly recommended. This section is important because it teaches students how to identify and be more aware of the deceiving methods that hackers love to use.

The third section gives students the ability to control someone's data on the Internet. The questions of this section give the students the ultimate experience of controlling someone's data on the Internet. This section consists of five questions. Each question is designed to enlighten students

on how users' information is handled and shared on the internet. In this section, some questions can be very sensitive but seeks to analyze college students' awareness level related to data privacy in regard to control of someone's data on the Internet. For example, a question asks "A department manager at a company has been directed by his boss to upload their client's information and share it with a third-party company. From a customer perspective, is this ethically wrong or morally right? These are the types of questions that will be given in the section to create an analysis. It puts subjects in the mind of having their information being shared with another user or third-party company without their consent. Furthermore, it enlightens students on the security issues related to protecting their data on the internet.

The fourth section of the survey is the participant information. This section is designed to give the researcher more valuable insight into the participants who complete the survey. In the last section of the survey, the participant has to answer the following questions: What is your trust level in regard to your organization or school protecting your data via the internet? What is your highest level of school you have completed or the highest degree you have received? What is your gender? What is your age? Are you White, Black or African American, American Indian or Alaskan Native, Asian, Native Hawaiian or other Pacific Islander, or some other race? Which best option applies to you: Computer Science related, or non-computer science-related. The answers from the participants' information will be used to analyze the distinguishing factors that make certain students aware of data privacy issues than those who are not.

3.5   Questions Design

The ultimate goal of the question was designed to create a real-life experience in a unique way without creating the hassle that reminds students that they are taking a survey. The questions simultaneously put students in real-life scenarios as they completed the survey.

3.6   Students Tested

We must continue to educate students on issues related to data privacy awareness. It's also critical that we continue to put more emphasis on data awareness as it pertains to our future. The survey was conducted on college students enrolled at Columbus State University (CSU). College students were chosen to be surveyed in the study because they are considered to be our future leaders. Therefore, in order to ensure data privacy awareness is being implemented throughout the world, we must instill a level of data privacy awareness amongst our college students. Additionally, more data privacy subjects should be taught more in educational institutions from the primary level to the college level. To attack some of these issues, there have been numerous colleges that have added a Data Privacy course to their curriculum. I hope the results from the college students surveyed in this study can mimic the world view.

3.7   Steps to Recruitment

Participants will be recruited through listserv and email. The researcher will send an invitation via to participants to participate. The email will introduce the researcher and provide an overview of the study. In addition, there will be an anonymous link that the participant can select or copy and paste into his or her internet browser to access the web-based survey. The first page of the web-based survey will include the following information: (1) an explanation of the research study and its purpose, (2) the research project's procedures, (3) a statement explaining no risks associated with the research project, (4) a statement explaining no benefits associated from the research project, (5) a statement explaining no compensation giving for participants, (6) a statement explaining confidentiality, and (7) a statement explaining the procedures for withdrawal. The

participants will select within the Survey Monkey web-based application as to whether they agree or disagree to participate in the study. If they choose not to participate, the survey will conclude, and the response will be recorded. If they choose to participate, then they will respond to each question in the survey.

3.8 Questionnaire Summary

The questionnaire was given to the students. Once completed, the answers were studied and analyzed based on each participant's result. The goal is to analyze whether college students were aware of the issues related to data privacy, as noted, and find the distinguishing factors that make certain students aware of those who are not. The questions of the questionnaire were divided into four parts: Data Privacy, Cryptography, The Control of Someone Data on the Internet, and Participant's information. In total, the survey consisted of 18 questions that each participant answered in order to fully complete the survey and used as part of the analysis. The basic design of the survey was formed to give subjects real-life experiences but also seek the importance of analyzing student's competence level as regards to the awareness on issues of data privacy. The questions were user friendly and formulated to put subjects in a position that reflects real-life experience without creating a hassle that reminds students that they are taking a survey.

4 RESULTS

4.1 Results and Score Grid

There were 104 participants who completed the surveys. Their results were collected through the SurveyMonkey database, a web-based survey service provider. The results were then analyzed to determine if the students were aware of the issues related to data privacy or not. In

order to evaluate each participant, a score was used to measure each participant's level. For the data privacy section, there were a total of 4 questions and the highest score that can be accumulated for the section was 8 points. For the cryptography section, there were a total of 3 questions and the highest score that can be accumulated for the section was 6 points. In the last section, control someone's data on the internet, there were a total of 5 questions and the highest score that can be accumulated for the section was 10 points. The most points a participant can obtain was 24 points. The 0-1-2 score differential score is the most valuable point system for this questionnaire. When measuring participants' data awareness level, it is highly suggested to provide participants with valuable feedback, and a researcher can only do so by measuring each their awareness level. In the event of a score of 1, it determines that the participants illustrated a minimal level of data privacy awareness. In the event of a score of 2, it determines that the participants illustrated a high level of data privacy awareness. Likewise, a score of 0 signifies no level of data awareness.

4.2   T-Test Distribution

For this thesis, a T-test Distribution is used in order to find the differential between the means of two groups. One set of data is compared to a different set of data. To test the two groups, the T-test function was performed in Google Sheets. To perform the function, the researcher typed the equal (=) sign into a cell and type 'TTEST' to start the formula. Once 'TTEST' is typed, an open parenthesis will appear, and the researcher must select the first set of data to be compared. Once the first set of data is selected then the researcher has to select the second set of data. Next, the researcher must enter the number '2' into the formula for the function to perform a two-tail test. Finally, the researcher needs to enter the number '3' to indicate that the two sets of data are unpaired. Once, the researcher encloses the function with a close parenthesis and presses 'Enter' then the p-value from the two sets of data will appear.

A p-value is used in hypothesis testing to help support or reject the hypothesis. If the p-value is less than 0.05 then there is sufficient evidence to support the hypothesis based on the p-value. Indicating that there is no difference between the means and conclude that a significant difference does exist. If the p-value is greater than 0.05 then there is insufficient evidence to support the hypothesis based on the p-value. Finding the p-value is one of the most frequently used measures for deciding if a result is statistically significant. In this study, the T-test provided a sampling size of the world's population of students by testing 104 of CSU's students.

4.3 Hypothesis

1. Females have a higher level of data awareness than males.

Females Means	Females Standard Deviations	P-Value
19.61	2.298	0.043

There is sufficient evidence to support the hypothesis based on the p-value of 0.043.

2. Whites have higher levels of data awareness than African Americans.

Whites Means	Whites Standard Deviations	P-Value
20.15	2.26	0.16

There is insufficient evidence to support the hypothesis based on the p-value of 0.16.

3. Whites have higher levels of data awareness than Asians.

Whites Means	Whites Standard Deviations	P-Value
20.15	2.26	0.40

There is insufficient evidence to support the hypothesis based on the p-value of 0.40.

4. Whites have higher levels of data awareness than students labeled as 'Multiple Races'.

Whites Means	Whites Standard Deviations	P-Value
20.15	2.26	0.73

There is insufficient evidence to support the hypothesis based on the p-value of 0.73.

5. African Americans have higher levels of data awareness than Asians.

African Americans Means	African Americans Standard Deviations	P-Value
19.48	2.11	0.72

There is insufficient evidence to support the hypothesis based on the p-value of 0.72.

6. African-Americans have higher levels of data awareness than students labeled as 'Multiple Races'.

African Americans Means	African Americans Standard Deviations	P-Value
19.48	2.11	0.82

There is insufficient evidence to support the hypothesis based on the p-value of 0.82.

7. Computer science-related students have higher levels of data awareness than non-computer science-related students.

Computer science-related Means	Computer science-related Standard Deviations	P-Value
23.08	2.13	0.01

There is sufficient evidence to support the hypothesis based on the p-value of 0.1.

8. Bachelor's students have higher levels of data awareness than high school graduates.

Bachelor's students Means	Bachelor's students Standard Deviations	P-Value
20	2.31	0.23

There is insufficient evidence to support the hypothesis based on the p-value 0f 0.23.

9. Bachelor's students have higher levels of data awareness than associate students.

Bachelor's students Means	Bachelor's students Standard Deviations	P-Value
20	2.31	0.13

There is insufficient evidence to support the hypothesis based on the p-value of 0.13.

10. Master's students have higher levels of data awareness than high school graduates.

Master's students Means	Master's students Standard Deviations	P-Value
20.33	2.13	0.08

There is quite insufficient evidence to support the hypothesis based on the p-value of 0.08.

11. Master's students have higher levels of data awareness than associate students.

Master's students Means	Master's students Standard Deviations	P-Value
20.33	2.13	0.23

There is insufficient evidence to support the hypothesis based on the p-value of 0.23.

12. Master's students have higher levels of data awareness than bachelor's students.

Master's students Means	Master's students Standard Deviations	P-Value
20.33	2.13	0.56

There is insufficient evidence to support the hypothesis based on the p-value of 0.56.

13. Students ages (18-24) have higher levels of data awareness than students ages (25-34).

Students ages (18-24) Means	Students ages (18-24) Standard Deviations	P-Value
20	2.30	0.34

There is insufficient evidence to support the hypothesis based on the p-value of 0.34.

14. Students ages (18-24) have higher levels of data awareness than students ages (35-44).

Students ages (18-24) Means	Students ages (18-24) Standard Deviations	P-Value
20	2.30	0.43

There is insufficient evidence to support the hypothesis based on the p-value of 0.43.

15. Students ages (18-24) have higher levels of data awareness than students ages (45-54).

Students ages (18-24) Means	Students ages (18-24) Standard Deviations	P-Value
20	2.30	0.27

There is insufficient evidence to support the hypothesis based on the p-value of 0.27.

16. Students ages (18-24) have higher levels of data awareness than students ages (55-64).

Students ages (18-24) Means	Students ages (18-24)	P-Value

	Standard Deviations	
20	2.30	0.14

There is insufficient evidence to support the hypothesis based on the p-value of 0.14.

4.4   Further Analysis based on Question #5

In contrast to the hypothesis, there seems to be a significant difference between races, ages, education levels, gender, and computer science-related when it comes to deciphering messages. Deciphering messages is a form of encryption. Even though presumably, some factors seem to put certain groups more favorable than others, understanding encrypting and decrypting messages presume to be otherwise. Question no. 5, asks students 'What is the Hidden Message of "VWXGHQW"? Students were asked to select one of the following answers as the correct encryption for the question. The selection of answers was 'GQWWHXV', STUDENT, 'WQHGXWV', or There is no hidden message. The question is pictured below in Figure 1: Hidden Message.

5. What is the Hidden Message of "VWXGHQW"
- GQWWHXV
- STUDENT
- WQHGXWV
- There is no hidden message

Figure 1: Hidden Message

The correct answers below are written in percentage evaluations in accordance.

1. In the hidden message of "VWXGHQW": Males have higher levels of data awareness than females?
   - 29.17% Males answered correctly vs 3.85% Females.

Males have higher levels of data awareness than females. This shows that males tend to be more sympathetic than females. In Figure 2: Males and Females Percentages, the graph shows the percentage of males answered correctly versus females.
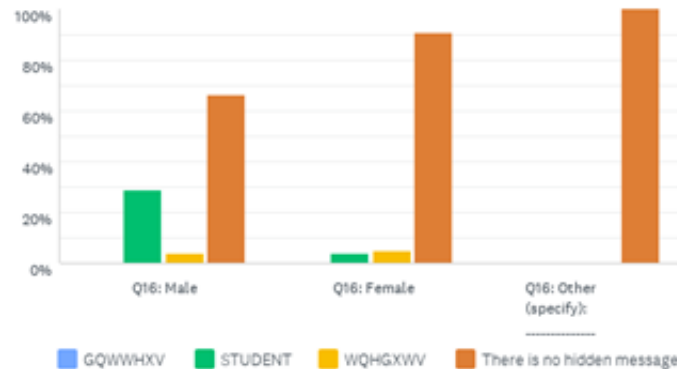

Figure 2: Males and Females Percentages

Below are more educated guesses based on Question 5. Below in Figure 3: Race Percentages, all the race responses appear.

2. In the hidden message of "VWXGHQW": Whites have higher levels of data awareness than African Americans?
   ○ 13.11% Whites answered correctly vs 0% African Americans

Whites have higher levels of data awareness than African Americans.

3. In the hidden message of "VWXGHQW": Whites have higher levels of data awareness than Asians?
   ○ 13.11% Whites answered correctly vs 0% Asians

Whites have higher levels of data awareness than Asians.

4. In the hidden message of "VWXGHQW": "VWXGHQW"? Whites have higher levels of data awareness than Native Americans?
   ○ 13.11% Whites answered correctly vs 0% Native Americans

Whites have higher levels of data awareness than Native Americans.

5. In the hidden message of "VWXGHQW": Whites have higher levels of data awareness than students labeled as 'Multiple Races'?
    ○ 13.11% Whites answered correctly vs 25% Multiple Races

Whites have higher levels of data awareness than students labeled as 'Multiple Races'.

6. In the hidden message of "VWXGHQW": African Americans have higher levels of data awareness than Asians?
    ○ 0% of Africans answered correctly vs 0% Asians

African Americans do not have higher levels of data awareness than Asians.

7. In the hidden message of "VWXGHQW": African Americans have higher levels of data awareness than Native American students?
    ○ 0% of Africans answered correctly vs 0% Native American

African Americans do not have higher levels of data awareness than Native Americans.

8. In the hidden message of "VWXGHQW": African Americans have higher levels of data awareness than students labeled as 'Multiple Races'?
    ○ 0% of Africans answered correctly vs 25% Multiple Races

African Americans do not have higher levels of data awareness than students labeled as 'Multiple Races'.
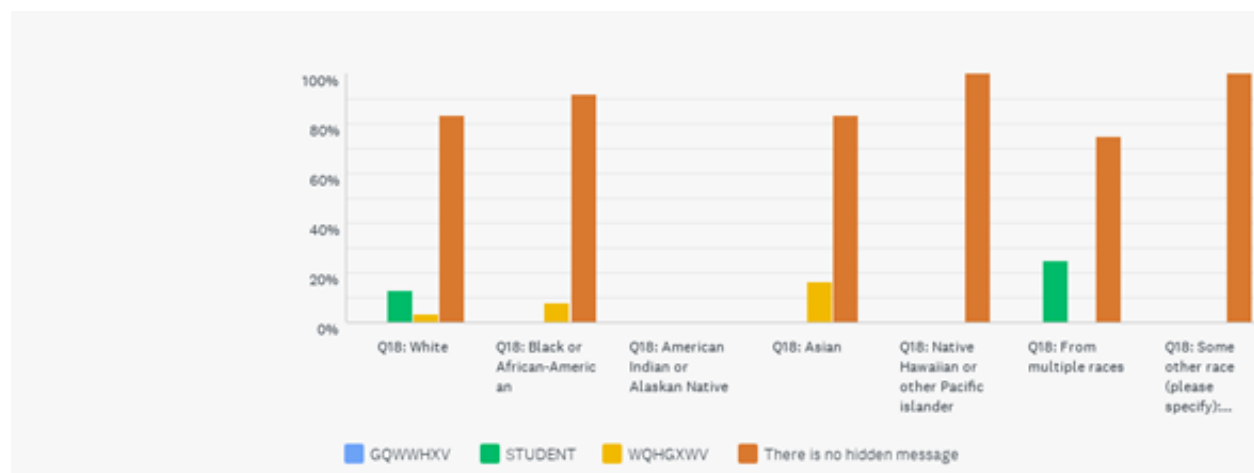

Figure 3: Race Percentages

Below are more educated guesses based on Question 5. Below in Figure 4: Computer Science and Non-Computer Science Percentages, all the computer science and non-computer science responses appear.

9. In the hidden message of "VWXGHQW": Computer science-related students have higher levels of data awareness than non-computer science related students?
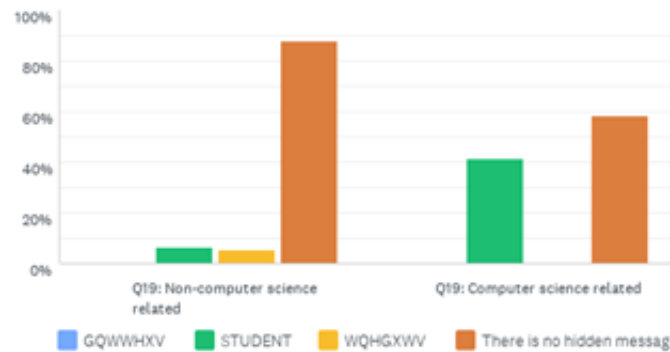   ○ 41.67% Computer Science answered correctly vs 6.52% Non-Computer Science

Computer science-related students have higher levels of data awareness than non-computer science related students.

Figure 4: Computer Science and Non-Computer Science Percentages

Below are more educated guesses based on Question 5. Below in Figure 5: Education Level Percentages, all the education level related responses appear.

10. In the hidden message of "VWXGHQW": Bachelor students have higher levels of data awareness than high school graduates?
    ○ 6% of Bachelor students answered correctly vs 1% of high school graduates

Bachelor students have higher levels of data awareness than high school graduates.

11. In the hidden message of "VWXGHQW": Bachelor students have higher levels of data awareness than associate students?
    ○ 6% of Bachelor students answered correctly vs 0% of associate students

Bachelor students have higher levels of data awareness than associate students.

12. In the hidden message of "VWXGHQW": Graduate students have higher levels of data awareness than high school graduates?
    ○ 3% of Graduate students answered correctly vs 1% of high school graduates

Graduate students have higher levels of data awareness than high school graduates.

13. In the hidden message of "VWXGHQW": Graduate students have higher levels of data awareness than bachelor students?
   ○ 3% of Graduate students answered correctly vs 1% bachelor students

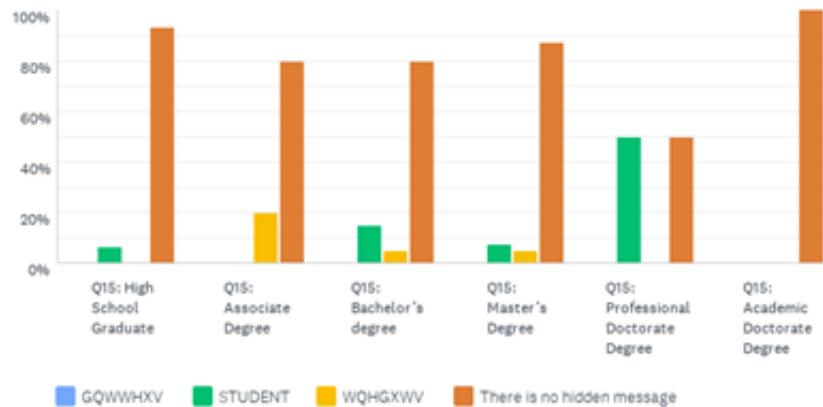Graduate students have higher levels of data awareness than bachelor students.

Figure 5: Education Level Percentages

Below are more educated guesses based on Question 5. Below in Figure 6: Age Percentages, all student age groups' responses appear.

14. In the hidden message of "VWXGHQW": Students ages from (18-24) have higher levels of data awareness than students ages from (25-34)?
   ○ 15.38% Ages (18-24) answered correctly than 9.38% Ages (25-34)

Students ages (18-24) have higher levels of data awareness than students ages from (25-34).

15. In the hidden message of "VWXGHQW": Students ages (18-24) have higher levels of data awareness than students ages from (35-44)?
   ○ 15.38% Ages (18-24) answered correctly than 6.25% Ages (35-44)

Students ages from (18-24) have higher levels of data awareness than students ages from (25-34).

16. In the hidden message of "VWXGHQW": Students ages from (18-24) have higher levels of data awareness than students ages from (45-54)?

○ 15.38% Ages (18-24) answered correctly than 8.33% Ages (45-54)

Students ages from (18-24) have higher levels of data awareness than students ages from (25-34).

17. In the hidden message of "VWXGHQW": Students ages from (18-24) have higher levels of data awareness than students ages from (55-64)?
   ○ 15.38% Ages (18-24) answered correctly than 0% Ages (55-64)

Students ages from (18-24) have higher levels of data awareness than students ages from (25-34).
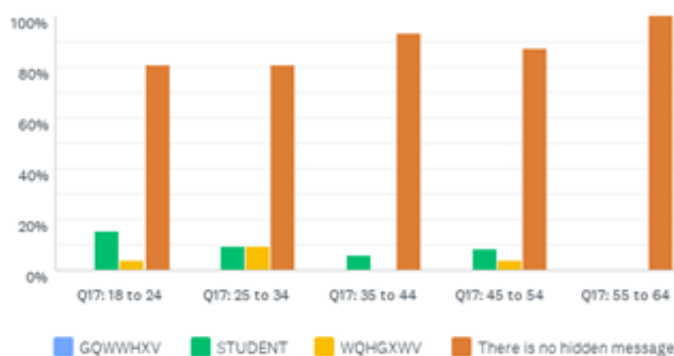
Figure 6: Age Percentages

5   CONCLUSIONS

This thesis aims for questionnaire-based survey research to analyze college students on the issues of data privacy. The structured questionnaire was uniquely designed to test students on their data privacy skills, cryptography skills, and their ability to evaluate how data should be handled and shared on the internet. The satisfactory results of the academic study sufficiently indicated that some college students were aware of the fundamental issues related to data privacy. The following hypotheses proved to be sufficient where females possess a higher level of data awareness than males. Females naturally tend to be aware due to their inner intuition while men become aware traditionally based on feelings. The following hypotheses proved to be sufficient where computer science-related students possess higher levels of data awareness than non-computer science-related

students. Computer science students invariably tend to have higher awareness levels because they are typically exposed to the potential threats of cybersecurity.

The further analysis section on Cryptography, based on Question #5, concluded that: (1) males answered correctly versus females, (2) Whites have higher levels of data awareness than African Americans, Asians, Native Americans, and Multiple races, (3) African Americans possess higher levels of data awareness than Native Americans and Multiple Races, (4) computer science related students possess higher levels of data awareness than non-computer science related students, (5) bachelor students possess higher levels of data awareness than high school graduates and associate students, (6) graduate students possess higher levels of data awareness than bachelor students, (7) students ages from (18-24) have higher levels of data awareness than students ages from (25-34), (35-44), (45-54), and (55-64). In conclusion, based on the p-values and percentages, it is clear that college students have some level of awareness in regard to data privacy.

6   LIMITATIONS

However, this study was limited based on the simplistic design of the questions from the survey. Even though the questions provide an in-depth analysis of data awareness amongst college students, there could have been more complex designed questions. The simplistic designed question was used as a beginning tool to analyze college students on basic data privacy issues. But as research shows, these real-life like questions are only the 'tip of the iceberg'. There are more trickeries that hackers use every day to manipulate individuals into stealing their information.

Overall, this study proved to be sufficient on the basic level. Hopefully, there will be another researcher that will create a more complex questionnaire in their study as it addresses this issue. This subject matter will be an ongoing issue and it's very important that students stay aware of the issues related to data privacy.

REFRENCES

A. Chaudhry, J. Crowcroft, H. Howard, A. Madhavapeddy, R. Mortier, H. Haddadi, and D.Mcauley, "Personal Data: Thinking Inside the Box," Aarhus Series on Human-Centered Computing, vol. 1, no. 1, p. 4, May 2015.

Ahola, M. (n.d.). The Role of Human Error in Successful Cyber Security Breaches. Retrieved July 17, 2020, from https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

Al-Janabi, Samaher & AlShourbaji, Ibrahim. (2016). A Study of Cyber Security Awareness in the Educational Environment in the Middle East. Journal of Information & Knowledge Management. 15. 1650007. 10.1142/S0219649216500076.

Andrews, V. 2019. Analyzing Awareness on Data Privacy. In Proceedings of the 2019 ACM Southeast Conference (ACM SE '19). Association for Computing Machinery, New York, NY, USA, 198–201. DOI:https://doi.org/10.1145/3299815.3314458

Alshboul, Y., & Streff, K. (2017). Beyond Cybersecurity Awareness. *Proceedings of the 2017 International Conference on Software and E-Business - ICSEB 2017*. doi:10.1145/3178212.3178218

B. Thuraisingham, "Big Data Security and Privacy," Proceedings of the 5th ACM Conference on Data and Application Security and Privacy - CODASPY 15, 2015.

Data Privacy - Definition & Types of Data. (n.d.). Retrieved from https://www.cleverism.com/lexicon/data-privacy/

Editor, M. (n.d.). What Can You Say When Your P-Value is Greater Than 0.05? Retrieved September 05, 2020, from https://blog.minitab.com/blog/understanding-statistics/what-can-you-say-when-your-p-value-i -greater-than-005

Hammarstrand, J., & Fu, T. (2015). Information security awareness and behaviour: of trained and untrained home users in Sweden.

Haukilehto, T. (2019). Improving Cyber Security awareness: Health, social services and regional government reform in South Ostrobothnia.

Help Net Security July 23, Help Net Security, & 23, J. (2020, July 23). Human error: Understand the mistakes that weaken cybersecurity. Retrieved August, 2020, from https://www.helpnetsecurity.com/2020/07/23/human-error-cybersecurity/

Hug, A. (2018). "I've got nothing to hide!". Proceedings of the 13th Workshop in Primary and Secondary Computing Education on - WiPSCE 18. doi: 10.1145/3265757.3265789

Kercher, K. E., & Rowe, D. C. (2012). Risks, rewards and raising awareness : training a cyber workforce using student red teams. *Proceedings of the 13th Annual Conference on Information Technology Education - SIGITE '12*. Association for Computing Machinery, New York, NY, USA, 75–8075-80. doi:10.1145/2380552.2380573

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. Management Research Review, 37(12), 1049-1092. doi:10.1108/mrr-04-2013-0085

Miller, M. (2020, March 26). Experts see over 600 percent spike in malicious emails during coronavirus crisis. Retrieved July 17, 2020, from https://thehill.com/policy/cybersecurity/489692-experts-see-over-600-percent-spike-in-malicious-emails-during

Mimecast. (n.d.). Malicious Email Attachments. Retrieved July 17, 2020, from https://www.mimecast.com/content/malicious-email-attachments/

Rainie, L., Anderson, J., & Connolly, J. (2019, December 31). Cyber Attacks Likely to Increase. Retrieved from https://www.pewresearch.org/internet/2014/10/29/cyber-attacks-likely-to-increase/

S. Phull and S. Som, "Symmetric Cryptography using Multiple Access Circular Queues (MACQ)," Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies - ICTCS 16, 2016.

Swinhoe, D. (2020, April 17). The 15 biggest data breaches of the 21st century. Retrieved July 17, 2020, from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Symanovich, S. (2020). Cyberattacks on the rise: What to do before and after a cyberattack or data breach. Retrieved from https://us.norton.com/internetsecurity-emerging-threats-cyberattacks-on-the-rise-what-to-do.html

T. (Producer). (2020, October 25). How to Calculate P-Value in Google Sheets! [Video file]. Retrieved from https://www.youtube.com/watch?v=u-IMEd1dmjM

The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. (n.d.). Retrieved August, 2020, from https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Two Sample t Test: Unequal variances. (n.d.). Retrieved September 03, 2020, from https://www.real-statistics.com/students-t-distribution/two-sample-t-test-uequal-variances/comment-page-1/

Udoh, E. S., & Alkharashi, A. (2016). Privacy risk awareness and the behavior of smartwatch users: A case study of Indiana University students. *2016 Future Technologies Conference (FTC)*. doi:10.1109/ftc.2016.7821714

Wright, D. (2018, November 21). How to State the Conclusion about a Hypothesis Test. Retrieved September 10, 2020, from https://www.drdawnwright.com/how-to-state-the-conclusion-about-a-hypothesis-test/

Warman, M. (2020, February 06). The world has changed. Digital has changed it. Retrieved August 19, 2020, from https://www.thedigitaltransformationpeople.com/channels/the-case-for-digital-transformation/the-world-has-changed-digital-has-changed-it/

Zidafamor, Emmanuel. (2018). A Study On Measuring Personel Cyber Security Awareness Level Through Phishing. 10.13140/RG.2.2.26372.68480.

APPENDICES
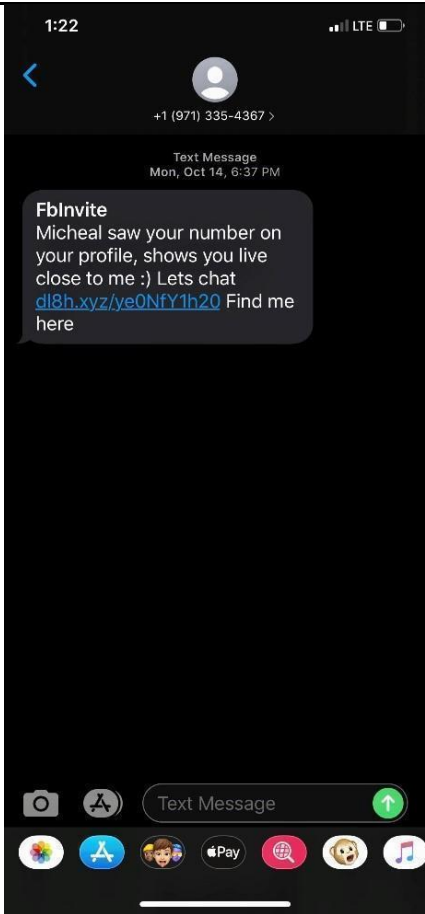
APPENDIX A - Old Questionnaire

<table>
<tr><td colspan="2">DATA PRIVACY:</td></tr>
<tr><td colspan="2">1. A data breach has occurred with your bank and your bank allegedly sends you an email. The email states that "we have recently been victims of a data breach and your account was hacked". The bank also states, "In order for us to ensure your privacy, enter your username and password below to change your password".</td></tr>
<tr><td colspan="2">

ENTER USERNAME

ENTER PASSWORD

● You will enter your information</td></tr>
<tr><td colspan="2">● You skip the email</td></tr>
<tr><td colspan="2">● You call to verify the email</td></tr>
<tr><td colspan="2">2. You received an email from your school, allegedly. The email informs you that your account has been temporarily locked and needs to be reset immediately. "Enter your credentials below and we will be notified to unlock your account".</td></tr>
<tr><td colspan="2">

ENTER USERNAME

ENTER PASSWORD

● You enter your credentials</td></tr>
<tr><td colspan="2">● You do not enter your credentials</td></tr>
<tr><td colspan="2">● You ignore the email</td></tr>
<tr><td colspan="2">3. You received a phone call stating "You are one of the luckiest winners and you have been qualified for a 3-day weekend trip to the Bahamas". The representative on the phone elaborates on how excited they are for you and convince you that this is a once in a lifetime opportunity. The representative then says you are allowed to use the trip within the next year only and you must have a credit card on file if you want to accept this 'once in a lifetime' offer.</td></tr>
<tr><td colspan="2">● You hang up the phone</td></tr>
<tr><td colspan="2">● You give the representative your credit card information</td></tr>
<tr><td colspan="2">● You ask for other promotion deals</td></tr>
<tr><td colspan="2">4. John opens his email account and scans through his inbox to find the email that his friend recently sent him. As John scans through his email, he notices an antivirus software scanner in</td></tr>
</table>

his email. Johns thinks to himself, "My computer has been downloading a lot slower and maybe I should give this a try". What should John do?

- Open the email and scan his computer to make it fun faster

- Do not open the email

- Continue searching for his friend's email

5. Sarah works at a help desk for a company. An employee calls and tells Sarah that her account is locked. The employee asks Sarah for her credentials because she has been in a tough meeting all morning and has forgotten her credentials. What should Sarah do?

- Give the employee her credentials of whom she says she is

- Verify whom the employee says she is

- Reset her credentials and give her the new temporary password

6. Mike accesses a non-secure site, but he is in a rush to meet a deadline. Mike knows the website is not secure. However, he assists on staying on the website.

- It is wise for Mike to be on the non-secure site to get the information he needs for his deadline

- Mike needs to hurry and finds what he is looking for then exit the site

- Mike needs to exit the site immediately

CONTROL SOMEONE'S DATA ON THE INTERNET:

7. Danny is a manager in the IT Department. Danny's boss asks him to look up their clients' information and send a copy of it to a third party. The third party wants to use the information for advertisement purposes. Danny immediately completes the task. From the customer's perspective, is this...?

- Unethical wrong

- Morally right

8. Geg.com is an exciting platform. You go to the account's website to see what the buzz is about. You decide to create an account, but first you read the terms of conditions. A line in terms of condition states "By creating an account, you give Geg.com the authorization to share and distribute your information as needed". So, you create an account and two months later Geg.com is exposed for sharing their clients' information with a third-party company. The third-party company designed a game model to sway the upcoming elections. You become worried and decide to contact Geg.com for answers. Geg.com informs you of the "fine line" in terms of conditions that you read before creating an account with them. You then say, "but I thought you would share my information with your customers on Geg.com and not with an outside party". Is this?

- Morally wrong

● The website's (Geg.com) fault
● Your fault

CRYPTOGRAPHY:

9. What is cryptography?
10. What is the Hidden Message of "FDW"? (Hint: Shift 3 left)
● CAT
● WDF
● IGZ
11. List the different forms of encryption:

APPENDIX B - New Questionnaire

DATA PRIVACY:
1. Micheal has been on the hunt for a job within the last few months and he has been really interested in building new relationships to potentially gain a new opportunity to land a job. On Monday at 6:37pm, he receives a text message from a number <u>9713354367</u>. The message reads (below): What should Micheal do?

- Click the link in the text to possibly meet his new dream job coworker. After all, Mike has been on the verge to meeting new connections, so he could land a job.

- Mike should ignore the message and just steadfast until the right opportunity comes along.

2. After a long workout at the gym, you head back to your locker to retrieve your phone. After retrieving your phone, you noticed that you have a missed call and voicemail from a number that you haven't seen before. You listen to the voice mails and it says "Hey what's going on I just wanted to touch base with you and see if you had a chance to finish reviewing the information for your online business. This is the one where you don't have to learn any marketing skills or talk to a bunch of people on the phone or close sales. The way the system is set up is you plug your information into it and you could be making you know around $9,000 - $10,000 a month and then we will show you how to make even more than that if you're really aggressive. I know you haven't had the chance to finish reviewing it from what it looks like but I know that it would not hurt you to check it out and I know there are a lot of

scams online so you want to definitely do your due diligence, but you might as well at least see what it's all about. It is 'www.your profit 247.com' and again that's 'www.yourprofit247.com.' It is spelled just the way it sounds thanks."

- Call the guy back and set up an account to become a sales representative. With the potentials of making $10,000 a month out of college is a once and a lifetime offer. Many people will be glad to be in your shoes and only wished it was them and not you, so you take the chance and chime in.

- It really seems to interest you, so you decide to do some research. You pull up google and search "yourprofit247.com".

3. You received a phone call stating, "You are one of the luckiest winners and you have been qualified for a 3-day weekend trip to Japan". The representative on the phone elaborates on how excited they are for you and convince you that this is a once in a lifetime opportunity. The representative then says you are allowed to use the trip within the next year only and you must have a credit card on file if you want to accept this 'once in a lifetime' offer. What would you do?

- Say, "No Thanks" but I will pass

- You give the representative your credit card information

- You ask for other promotional deals

4. A data breach has occurred with your Car Insurance company and your Car Insurance company allegedly sends you an email. The email states that "we have recently been victims of a data breach and your account was hacked". The Car Insurance company also states, "In order for us to ensure your privacy, enter your username and password below to change your password". What would you do?

ENTER USERNAME

ENTER PASSWORD

- Enter your credentials

- Call to your Car Insurance company to verify the email

CRYPTOGRAPHY:

5. What is the Hidden Message of "VWXGHQW"

- GQWWHXV

- STUDENT

- WQHGXWV

- There is no hidden message

6. Define cryptography?
7. List any different types of encryption
CONTROL SOMEONE'S DATA ON THE INTERNET:
8. Roger has been giving orders from his boss to share their customers data with EyeScape Inc. EyeScape Inc. is known for being one of the most innovative marketing companies in the world. However, Roger is an expert in his field and is highly aware that passing this data on to EyeScape Inc is considered a violation to their customers' data privacy, so Roger completes the task. From a customer perspective, is this?
● Morally right
● Unethical wrong
9. Matt is a manager in the IT Department. Matt's boss asks him to look up their clients' information and send a copy of it to a third party. The third party wants to use the information for advertisement purposes. Matt immediately completes the task. From the customer's perspective, is this...?
● Unethically wrong
● Morally right
10. Would you share someone's personal information with others via the internet?
● Yes
● No
11. How often are you exposing your personal information on the internet?
● Often but for personal uses
● Not often
12. Geg.com is a new, upcoming exciting platform. You go to the account's website to see what the buzz is about. You decide to create an account, but first you read the terms of conditions. A line in the terms of conditions states "By creating an account, you give Geg.com the authorization to share and distribute your information as needed". So, you create an account and two months later Geg.com is exposed for sharing their clients' information with a third-party company. The third-party company designed a game model to sway the upcoming elections. You become worried and decide to contact Geg.com for answers. Geg.com informs you of the "fine line" in terms of conditions that you read before creating an account with them. You then say, "but I thought you would share my information with your customers on Geg.com and not with an outside party". Is this?
● A mistake on your behalf
● A mistake on Geg.com
Participants' Information

13. What is your trust level in regard to your organization or school protecting your personally data via internet:

- Highly Trustworthy

- Semi Trustworthy

- Not Trustworthy

- Have not considered it yet

14. What is your highest level of school you have completed or the highest degree you have received?

- High School Graduate

- Associate Degree

- Bachelor's degree

- Master's Degree

- Professional Doctorate Degree

- Academic Doctorate Degree

15. What is your gender?

- Male

- Female

- Other (specify): _____

16. What is your age?

- 18 to 24

- 25 to 34

- 35 to 44

- 45 to 54

- 55 to 64

17. Are you White, Black or African-American, American Indian or Alaskan Native, Asian, Native Hawaiian or other Pacific Islander, or some other race?

- White

- Black or African-American

- American Indian or Alaskan Native

- Asian

● Native Hawaiian or other Pacific islander
● From multiple races
● Some other race (please specify): _____
18. Select the best option that applies to you:
● Non-computer science related
● Computer science related