Spring 3-2021

Cybersecurity Education for Non-Technical Learners

Matthew McNulty
Dakota State University

Cybersecurity Education for Non-Technical Learners

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Cyber Operations

March 2021

By

Matthew McNulty

Dissertation Committee:

Dr. Kyle Cronin

Committee Chair

Dr. Crystal Pauli

Committee Member

Dr. Tom Halverson

Committee Member

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Matthew McNulty

Dissertation Title: Cybersecurity Education for Non-Technical Learners

---

Dissertation Chair/Co-Chair: Kyle Cronin Date: May 3, 2021

Name: Kyle Cronin

Committee member: Crystal Pauli Date: May 3, 2021

Name: Crystal Pauli

Committee member: ________ Date: May 3, 2021

Name: Tom Halverson

Original to Office of Graduate Studies and Research
Acid-free copies with written reports to library

ABSTRACT

Today's world is increasingly reliant on technology for school, work, entertainment, and general home use. Many jobs today could not be performed without the use of computer systems or other technology. As lives become intertwined with technology, everyone will inevitably encounter malicious, vulnerable, or privacy-compromising devices or services. Unfortunately, knowledge of how to deal with these cybersecurity and privacy issues is not something that falls within the domain of common knowledge for the everyday person. Additionally, there is a lack of work being done to understand the educational needs of various groups within the general public and educate them. This quantitative survey research study seeks to add to this knowledge base by looking to better understand what university students at the Southeastern Louisiana University comprehend regarding cybersecurity and privacy protection best practices and associated standard technologies. Furthermore, this work will examine whether the student's academic major has any effect on their responses.

This research examines the responses from university students to a survey using non-technical questions in cybersecurity, privacy protection, and some standard, related technologies. The combination of answers to these questions and the major given by the student provides conclusions of what is common knowledge for the university population and if their major had any effect on their ability to answer the questions correctly.

Based on 810 responses to the survey, it can be concluded that there are participants who are unsure or incorrect in their knowledge of a given idea for any of the examined subjects. Additionally, majoring in computer science or information technology results in students having an increased likelihood to answer correctly. Students in these majors do show a lower rate of

providing an incorrect answer, but it does not eliminate the deficiencies. The research shows that education for all students in cybersecurity, privacy protection, and related technologies is needed. Finally, while some solutions are presented, additional research is required to educate them further.

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotations marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

Matthew McNulty

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Today's world is increasingly reliant on technology for school, work, entertainment, and general home use. Many jobs and other activities today simply cannot be performed without the use of computer systems and other technologies. Course content is delivered to students through online programs as supplements and entirely online courses in education systems. Entertainment and other home devices have become internet-connected devices with televisions, computers, voice assistants, and any number of smart devices being connected to the internet to access their full features. Additionally, online options for payments and many other needs have become available in most industries. In all aspects of an individual's life, technology continues to have a growing foothold.

With this idea in mind, as lives become intertwined with technology, everyone will inevitably encounter malicious, vulnerable, or privacy-compromising devices or services (Dupuis, 2017; European Union Agency for Cybersecurity [ENISA], 2020). Since it is more of a certainty that this occurs rather than if it happens, everyone needs to have a level of education to protect both their devices and private information. Protecting devices and information becomes increasingly important when one individual is working with another individual's private information. Unfortunately, a complete understanding of common best practices cannot yet be called common knowledge. So there is a need to look for ways to educate individuals outside of a specialized education program for these areas that could give them this knowledge (Dupuis, 2017; McNulty & Kettani, 2020).

The following dissertation research project explores the knowledge and understanding of cybersecurity and privacy practices and some common technologies that surround them. The studied population is college students at Southeastern Louisiana University in the Fall of 2020. This research yields information regarding the knowledge level of the students in attendance during that semester and makes recommendations on possible ways to increase this base knowledge level.

In this chapter, a background of the topic is given, which leads to the problem statement by discussing the basis of the issue surrounding the area of research. The statement of the problem and purpose of the study provide information on the reason and goal of this research. A set of research questions and null hypotheses are given to help further show the driving goal of the study. Finally, the remainder of the chapter is dedicated to the nature of the study and those who would be involved in it.

Background

Today every individual has a growing exposure to devices that are connected to a network. Whether their devices are some of the more standard, everyday ones, such as a laptop or a smartphone, or a device from the growing trend of connected Internet of Things (IoT), that could include everything from a smart power outlet, a voice-activated assistant, all the way to an entire home monitoring system, there is an ever-growing chance that an individual will be using some type of connected device each day (Davis, 2015). As the device and workspace landscape continues to change, the threats to these devices also change. The annual reports from the European Union Agency for Network and Information Security (ENISA) and the yearly and monthly reports from Symantec all can show us that while the prevalence of certain types of threats and the trends of others may change, the fact remains that there is a multitude of threats that are out there (ENISA, 2020; Symantec, 2019a, 2019b).

In addition to the threats themselves that individuals face, there may be many cases where they are unaware that any problem has occurred. Without knowledge of proper techniques for preparing for when their information gets leaked, that person may be at even greater risk. In 2019, the Office of the Australian Information Commissioner (OAIC) published a report on their findings from the first year of their Notifiable Data Breaches (NDB) scheme being mandatory (Office of the Australian Information Commissioner [OAIC], 2019). The NDB scheme required businesses and government agencies to notify the OAIC and "carry out an assessment whenever they suspect that there may have been loss of, unauthorized access to, or unauthorized disclosure of personal information that they hold" (OAIC, 2019). The mandatory reporting caused a 712% increase in notifications in the initial 12-month period (OAIC, 2019). From this, it can be inferred that many data breaches would have otherwise gone unreported and thus likely remained unknown to those affected. Even with proper reporting and response, it can take time to discover and deal with a breach. In 2020, the average time to identify and deal with a breach was 280 days (IBM Security & Ponemon Institute [IBM], 2020). This changing landscape shows the need for a flexible education curriculum that can be constantly changed and kept up to date. Changing the curriculum based on current events would allow it to follow the latest information and trends as closely as possible as these changes occur and not become mired in outdated information (Dreibelbis, 2016). By keeping up-to-date, individuals are given the best opportunity to protect themselves even when they are part of a data breach and may not be notified for some time, if at all.

Problem Statement

For the general person, best practices for cybersecurity and privacy protection are topics that cannot be said to be common knowledge (Robot, 2016; Paulsen et al., 2012). This fact means that there are active threats to individuals, their families, and their organizations that they are not equipped to deal with (Dupuis, 2017; Olmstead & Smith, 2017). Even something as simple as the games that an individual, regardless of age, chooses to use can end up being less benign than they might believe (Cox, 2019; Valentino-DeVries et al., 2018). There could also be incidental leaks in the method software companies use to improve that same software, such as with Skype used by individuals and businesses alike (D'Anastasia & Mehrotra, 2019).

There is a lack of literature exploring many groups' awareness of cybersecurity and privacy protection practices and technologies. While not completely devoid of any research, some groups have not been properly assessed or lumped in with other groups (Dupuis, 2017; Olmstead & Smith, 2017).

This study seeks to address the fact that the average college student is not receiving an adequate education in cybersecurity and privacy protection practices if they are not within a major that would directly expose them to these concepts. To look more closely at this issue, a survey was employed to gauge the level of knowledge of college students at Southeastern Louisiana University in cybersecurity and privacy practices and common technologies employed in both areas. To accomplish the survey, a portion of the student population was surveyed for what they knew about several important but generalized areas in these realms. The goal was to obtain a quantitative measurement of this student population's knowledge level and what areas are more commonly understood than others within what the survey would be able to gauge. For the purposes of this study, the term non-technical will be used to identify an individual who is outside of a computer science, information technology, or related discipline.

Purpose Statement

The study examines several key areas of cybersecurity and privacy best practices and seeks to gauge a generalized knowledge level to the target population. Since the study looks to place a value on the knowledge level of college students, a quantitative methodology was used (Creswell, 2014). This methodology allows the study results to be quantifiable and used as a basis for further study, thus contributing to more focused and generalizable research in this field.

To properly assess the knowledge of the student population, a survey was designed to ask the participants to answer questions, to the best of their ability, in several simplified areas relating to cybersecurity, privacy protection, and some common technologies used by many individuals outside of those fields. A non-technical approach was taken to form the questions and their answers so that the required knowledge to participate in the survey fully would be at a minimum. This non-technical approach is important due to the nature of the study and its participants. The wide range of knowledge that students may already have does provide an unknown variable for the research. However, that fact fits in line with the research goal to understand what knowledge or ideas are more common than others. More information on the participants, the study itself, and its scope are detailed later in this chapter.

Quantitative Research Questions and Hypotheses

As given in the purpose statement, the study employed a quantitative research method to properly assess the level of knowledge in cybersecurity and privacy best practices for college students. So that the knowledge levels of the surveyed areas and a comparison between those in a technical major versus a non-technical major could be examined, two research questions were given as:

Q1. How familiar with basic concepts in cybersecurity and privacy best practices are college students at the Southeastern Louisiana University?

Q2. Does an individual in a technical major have a higher base knowledge level than an individual in a non-technical major?

To follow along with these questions, the following two null hypotheses were proposed:

$\mathbf{H1_0}$**:** Students at the Southeastern Louisiana University are very familiar with the examined practices.

$\mathbf{H2_0}$**:** The major that a student has chosen does not affect their knowledge in the areas of cybersecurity and privacy.

Significance of Study

While several entities can allow for an education program to show a certain level of rigor in what it is offering its students in cybersecurity, computer science, or related technology-centric programs, such as the Accreditation Board for Engineering and Technology (ABET) or the National Security Agency's (NSA) Centers of Academic Excellence (CAE), there is nothing that sets a standard for what of, if any, information of this type should be taught to those who are in disciplines outside of these programs or outside of the education levels that these programs are looking at (Accreditation Board for Engineering and Technology[ABET], n.d.; Dupuis, 2017; National Security Agency[NSA], n.d.). While some locations are attempting to implement cybersecurity and privacy protection-related education at many different levels, these programs are not unified in the materials they attempt to get across to their learners (Mache & Weiss, 2018; Pye, 2016; Schwartz, 2018; Skinner, 2017). Additionally, they are not always consistent in how information is presented (Katasantonis, Fouliras, & Mayridis 2017). This inconsistency can lead to drastically different outcomes for the learners (Abd Rahim et al., 2015). Additionally, since not all learners are at the same level, the need to adjust the type of learning materials presented and their contents to the audience must be considered.

Since each audience should be considered separately, then a single solution is not applicable across all learners (Abd Rahim, 2015). Different people will learn at different rates and have different base knowledge levels (Furman et al., 2012; Hoggard, 2014; Scheponik et al., 2016). Thus, the need for more general and for more targeted research to take place. This need for more targeted research, with this study looking at college students, is the main contribution that this research seeks to make. By examining the knowledge level of the students at the Southeastern Louisiana University and getting a base here, then further work can be done to expand this area of targeted research and more generalized studies.

Nature of the Study

The following section describes the participants involved in the study and considerations for the creation of the survey, the type of data being collected, the scope of the research, and any assumptions made.

Participants. The target population used for the survey was Southeastern Louisiana University students who are over the age of eighteen. No restrictions on classification or major were imposed, and not placing restrictions on these areas allowed for a good cross-discipline set of responses from individuals who will be entering the workforce in the near future. The participants were a random sampling of all students currently attending the university as of Fall 2020.

The Survey. The survey itself was looking to find the overall knowledge level of the students. By examining how much knowledge the average person from the sample population possesses within the different basic ideas presented, the overall population's level of understanding can be explored. By looking at the number of correct responses, a general idea of this level can be gained. Additionally, individuals may believe they possess correct ideas when they have misconstrued ideas in how they believe a piece of technology works. It was important to gauge the actual understanding of the sample population in some areas instead of just a simple right or wrong. With these first two ideas, it can be seen how well the general population at the university understood what was presented to them, if there were deficiencies, or if there were misconceptions. Overall, the hypothesis that this survey was looking to prove or disprove is that individuals do not understand the basics of cybersecurity and privacy protection and associated technologies that are needed for today’s technological world.

Scope. The scope of the survey was limited to current university students at Southeastern Louisiana University. This limitation means that the survey did not consider individuals who are already in the workforce, who may have different priorities than students, nor consider students who are still in the K-12 education system. The survey will be generalized to the study body of the university. However, further generalization to the college population at the state or country level is outside the scope of this research.

Ethical Considerations. No identifying information was gathered to be used for the survey. Participants were still asked to enter some of their personal information such as age, gender, classification, and major as part of the survey. However, it is important to note that identifying participants would not be possible given the nature of the data.

The main ethical concern is that the principal researcher is currently an instructor at the university where the study was performed. It was made clear that no academic advantage or penalty would be given for participation, or non-participation, in the survey such that no student would feel pressured if they happened to be in a course taught by or in the same department as the researcher.

Assumptions. There are a few assumptions made for this research study. The first is that each individual taking the survey will be a student at the Southeastern Louisiana University. Since their university email account will be used to contact them, this is a fairly safe assumption. Still, since alumni are allowed to keep and use their email account after graduation, it is something to consider. A second assumption is that the surveyed population will be representative of the entire university population. While different majors may have different general concerns, with the interconnectivity afforded by the internet and online media, this assumption for students that come from many different areas of study should still provide a good representative sample of the overall university. However, as mentioned above, it is not assumed that the population can represent their peers in other areas of the country. Finally, it is assumed that there is basic computer literacy to take the survey. Each participant will need to use a password to log into their email to receive the survey information and access the survey itself in a web browser. While there may be topics on the survey itself that they may be unfamiliar with, that is in line with its intended design so long as they are competent enough to access the survey properly.

Definitions

The following terms are defined so that the reader can have a consistent view of what is intended by their usage regardless of background or experience. For these definitions, the capitalizations do not affect their usages throughout this work.

Non-Technical: For this work, non-technical will refer to individuals who are not within a computer science, information technology, or similar degree program.

Cybersecurity: In the context of this work, cybersecurity refers to the general field of study surrounding the protection and prevention of an unauthorized entity gaining access to a computer system or data that they otherwise would not have access to use or see.

Privacy/Private Information: The ability of an individual or corporation to have control over information that could be used to identify them, their habits, or other confidential information such as social security number, credit card information, or medical records.

Encrypted: Information is considered encrypted if it is no longer in its original form such that only the originator and the intended recipient of a message should be able to understand it, not a third party.

HTTP: HTTP stands for Hypertext Transfer Protocol and is how data is transferred across the world wide web.

HTTPS: The addition of the 'S' adds "Secure" to HTTP. This addition lets us know that the connection automatically encrypts the data transferred through it over the internet.

Private Browsing: This is a feature found in most modern internet browsers. Typically, the most common use cases for entering private browsing mode are that users do not wish their current session using that browser to be remembered in the browsing history.

VPN: A Virtual Private Network can be used to make it appear as if data is sent to a website or another online outlet is coming from a different location than where you are located. The typical usage is that an individual will connect to a VPN service, then all of their internet traffic will appear to be coming from their VPN host rather than their computer to any point after the VPN's server.

Embedded: For the study, embedded refers to information being encapsulated within another piece of data. For example, the time that a photograph was taken could be within the data of that photograph and not physically shown.

Malware: Any program that is not performing to the expectations of the user. This could be malicious behavior, the undisclosed gathering of information, or attempts to install unwanted software.

Chapter Summary

In this chapter, the problem being addressed by the research was presented to the reader. The issues surrounding the growing trend of internet-connected devices and a user population not adequately educated in the dangers posed by those devices were introduced. A prosed quantitative methodology study was outlined with the research questions and null hypotheses being tested were given. Information regarding the survey used, its target population, scope, and other considerations in its design were outlined. In the coming chapters, a more thorough review of existing literature in this area is examined. Further information on the research methodology is given, the results of the survey are provided, and then conclusions drawn from the results and recommendations are made.

CHAPTER 2

LITERATURE REVIEW

Knowledge of cybersecurity concepts surrounding the protection of personal and other online information is a key aspect of our increasingly connected world. However, getting the know-how of what to do to protect one's self, family, and business is not a straightforward process for many individuals. This is especially true for those who are not in a technically focused education program, where this research focuses.

While there are programs designed to give individuals a chance to obtain the necessary information they need, there is a lack of consistency. However, there are initiatives working to help with this issue. This can be seen at several different levels. Often, the information being given is heavily dependent on the individual who created the program or the reason behind creating it. In either case, most of the time, the curriculum or how the curriculum was created is not shared information.

The following literature review process looked at the information and programs available to determine what areas have been explored. It also looks at what the various programs and program types are covering. Finally, what research has already been done is examined to determine the level of cybersecurity knowledge for the average person at or approaching the university level.

Existing Work

In 2016, President Barack Obama issued an Executive Order on the growth of cybersecurity at the national level. Section three, subsection a, point five, states a goal of "improving broad-based education of commonsense cybersecurity practices for the general public" (The White House, 2016). However, there is still not a lot of research on the actual education of the public.

Much of the existing research focuses on the need to train professionals in cybersecurity or related disciplines rather than expanding the knowledge base of individuals who are not attempting to learn about these areas directly (ENISA, 2020). While some research is in the appropriate areas, it is not as consistent as agencies that specifically deal with those areas.

The entities mentioned in the previous chapter, ABET and the NSA's CAEs, give accreditations to programs in various specialized areas (ABET, n.d.) or specifically geared toward cybersecurity (NSA, n.d.). Additionally, there are standards set for various roles that can be found within the cybersecurity and technology workforce through the National Institute of Standards and Technology (NIST) and the National Initiative for Cybersecurity Education's (NICE) framework (Newhouse et al., 2017; Paulsen et al., 2012). However, these do not address a majority of the population.

General Public

Actual awareness of how to deal with many threats cannot be considered common knowledge (Dreibelbis, 2016; McNulty & Kettani, 2020; Olmstead & Smith, 2017; Robot, 2016). Whether it is something as simple as a phishing email or knowing how to deal with malware or another cyber threat, the top of which is reported on by bodies such as ENISA or Symantec, the average person needs to know what to do to deal with these threats. Additionally, these threats are not the only ones that could be represented as online dangers. Depending on the nature of the audience, cyberbullying could be just as big of a threat as a piece of malware stealing banking credentials (Pye, 2016; Schwartz, 2018; Skinner, 2017). The wide range of people in all age groups who are vulnerable at home and work compounds the difficulty of relaying relevant information to each individual. Behavioral aspects must also be considered to accurately delve into how individuals will respond to cybersecurity information presented to them (Furman, 2012).

While many are interested in and realize the importance of this type of education, the actual time or monetary cost can cause issues with the actual delivery. Many adults with children in the middle to high school range were found in this study to realize the importance of educating themselves and their families. Still, they would only be willing to devote sixty to ninety minutes towards a seminar on it, and around 40% of the participants were not willing to pay for it (Ricci et al., 2018). This result shows that importance is less of a factor and a good reason for including it as early as possible into the education system.

K-12 Education

There is research on attempts to implement various levels of education in the K-12 section of the education system (Cyber Innovation Center [Cyber], n.d.; Pye, 2016; Schwartz, 2018; Skinner, 2017) or to find out how willing other groups would be to seek education (Ricci et al., 2018). Additionally, some research focused on cybersecurity students' understanding of various concepts within the cybersecurity discipline. While not wholly applicable to this research, it can show that even students attempting to learn the discipline can still misinterpret concepts or conflated ideas (Scheponik et al., 2016; Thompson et al., 2018). Some locations are attempting to implement cybersecurity and privacy protection-related education at many different levels. These programs are not unified in the materials they are attempting to put across, nor are they always consistent in how information is presented (Abd Rahim et al., 2015). This can lead to drastically different outcomes for the learners. Additionally, the landscape of threats in the cybersecurity realm is constantly changing, meaning that this fact needs to be considered when creating these programs.

High School Students

There are only a few school districts that are attempting to implement some type of cyber awareness program for students around the high school grades. From what has been seen, the program usually comes from an individual who has taken a personal interest in beginning the program rather than a larger initiative (Pye, 2016; Schwartz, 2018; Skinner, 2017). This type of disparate approach can lead to different materials being used for educating these students. In turn, this can cause the actual effectiveness of the approach to be entirely dependent on the outlook of just the individual that has been placed in charge of the initiative or is the person attempting to get it started. There is also the potential for a bias to be introduced that could lead to the material being covered as relevant to just a specific type of threat or type of student rather than being generic enough to be applicable by everyone in all situations. The Cyber Innovation Center does have an academic initiative in Cyber.org that revolves around giving educators a common set of tools to work with for teaching students cyber education (Cyber, n.d.). These resources do focus more on providing education in cybersecurity itself rather than non-technical best practices. However, even if a student decides not to stick with cybersecurity after taking a course over the information, it would still benefit them. This will be discussed in more detail later in the chapter.

College Students

For students in the college system, if they are not within a technical major, many will still not come into contact with these topics despite the concepts being very useful for their time at school and their eventual time in the workforce (McNulty & Kettani, 2020). Much of the burden for this section of students would fall onto both the college, to offer at least a course instructing the students in the fundamentals of cybersecurity and privacy protection, and on accrediting bodies to push colleges into having this as part of the requirements for being accredited (Dupuis, 2017). This would be similar to, as an example, the requirement of a specific number of sociology hours for all students. In either case, the more students can learn about the methods to protect themselves from cyber threats, the less burden will fall on professionals to provide that protection (ENISA, 2020). In the end, the user is still responsible for much of the loss of information or malware infections (Symantec, 2017; OAIC, 2019). That is not to say that it is the victim's fault for falling for some type of scam or attack, but rather that it is evidence that additional education on how to avoid and deal with them is necessary. While there are tools available for network administrators or other technology-related staff to mitigate these threats as much as possible, they still are not perfect. Some active threats that can be viewed from the university level will be explored later in this chapter. Additionally, in this chapter, two studies that included college-age individuals will be examined in more detail.

Preparing Students

While traditional education offerings for a generalized, non-technical cybersecurity education are minimal, there are other places that can be looked to where a student might receive some knowledge in these areas. One such place is summer camps and similar programs. Even though many of these offerings that are in cybersecurity, computer science, or other STEM discipline are focused on the recruitment of students into those fields, their teachings can still be leveraged by all students to gain a better understanding of related concepts (Achee, 2021; CybHER, n.d; Dark et al., 2021; Divito, 2017; GenCyber, n.d.; Raigoza, 2018; Rowland et al., 2018). Even if the students who attend these camps do not end up in the field of study that the camp was aimed at, it can still provide them a good baseline education into areas that they may not otherwise have had access to (Dark et al., 2021). Additionally, these camps can be held for students of any age range, up to and including those who are about to enter college (Achee, 2021; Divito, 2017, GenCyber, n.d.; Raigoza, 2018; Rowland et al., 2018). While the camps examined here have a cybersecurity or computer science focus, the same ideas presented could be applied to other types of short-term camps to teach basic cybersecurity concepts outside of the educational system in addition to their normal activities.

The general goal of these camps is to better prepare students in the subject matter that the camps cover and interest students in those areas to move forward. The hope then is that they are motivated to either keep educated in the area or to choose that subject as a part of or a whole of their school or career path (Achee, 2021; Dark et al., 2021; Divito, 2017; GenCyber, n.d.; Raigoza, 2018; Rowland et al., 2018). The exact subject areas, methods, and targeted groups may vary, but those goals remain consistent. Even if the recruitment aspect is removed from the camps, the actual knowledge advancement benefits the students who can participate (Dark et al., 2021). So, even if it is assumed that a student does not stay in the given subject area of a particular camp, they still received the information from attending that camp. That education could still help shape their future actions, even if it isn't to stay within the field. This is where including basic cybersecurity and privacy best practices into a camp in some fashion could be a large boon for any student that attend, even if they do not stay in a directly related field.

These camps' outreach gives opportunities that many individuals would otherwise not have had to participate in these subject areas (Dark et al., 2021; Raigoza, 2018). In this, the goal of educating students in cybersecurity and privacy can align with any camp. Those are also subject areas in which not many individuals have an opportunity to participate. These camps can also be targeted to multiple age ranges or aimed at specific groups of individuals to better fit their subject matter to their audience (Achee, 2021; Divito, 2017; Raigoza, 2018; Rowland et al., 2018).

This flexibility allows for students who are about to or have completed high school to be better prepared for what is coming as they transition to their college career (Achee, 2021; Dark et al., 2021; Divito, 2017; Raigoza, 2018). These ideas can be applied to a wide range of different subjects. By engaging with the students before they enter their first semester of classes, they can be better prepared for what is expected of them and what will come (Achee, 2021; Divito, 2017; Raigoza, 2018). While not a guarantee that they will stay with the subject areas, it can be the first step in giving them a group to learn and work with if they continue (Raigoza, 2018). Additionally, it can show that others are also facing the given information for the first time and help ground these ideas in personal experiences. Additionally, these camps can also be aimed at younger students who have not yet reach high school but still need to be made aware of many types of issues or shown what opportunities are available to them (CybHER, n.d.; GenCyber, n.d.; Rowland et al., 2018).

However, the reach of such camps is limited (Achee, 2021; Dark et al., 2021; CybHER, n.d.). How many students they can reach depends on a great number of factors. Some of these factors include costs to both the camp itself and its participants, size restraints, and availability (Achee, 2021; CybHER, n.d., Raigoza, 2018). A monetary cost can be a limiting factor for both the camp and participants. If a camp is keeping students for much of the day, food would need to be provided, and if a camp allowed students to stay on-site for a multi-day camp, then lodging would need to be made available. Both of these things will have a monetary cost associated with them (Raigoza, 2018). While this can be offset with outside funding, such as GenCyber that aims to offer such camps at no cost to participants, some camps may need to pass along the costs, at least in part, to those wishing to attend (GenCyber, n.d., Raigoza, 2018). As previously shown, a monetary cost to the participant is a large detrimental factor for willingness to participate (Ricci et al., 2018). Another factor that severely limits the impact that many camps can have is simply the available space for students. For their 2021 camp, the CybHER Girls camp that targets students in the Midwest has a limit of 75 students (CybHER, n.d.). In the camp mentioned by Achee, in 2020, it had an increased limit of 80 that filled within the first 72 hours and gained a waitlist of 100 students before it was capped (Achee, 2021). Both of these show that there are opportunities available. However, they may be limited and fill quickly. Finally, the biggest limiting factor is simply availability in a given area, though virtual camps could help that somewhat (Achee, 2021).

GenCyber, as mentioned previously, is an organization that works to “provide summer cybersecurity camp experiences for students and teachers at the K-12 level” (GenCyber, n.d.).

However, the organization can only provide funding opportunities to a limited number of camps, with their funding from the National Security Agency (GenCyber, n.d.). While the funding of camps is great, their limited reach can be seen in their reported numbers. In a 5-year evaluation of the program that spanned 2015 to 2019, it was reported that 15,545 students attended GenCyber in that period (Dark et al., 2021). Of those, 7,160 graduated from high school and participated in the evaluation study (Dark et al., 2021). However, according to the U.S. Bureau of Labor Statistics, in 2019 alone, 3.2 million individuals graduated from high school (U.S. Bureau of Labor Statistics, 2020). This can help put into perspective the difference in volume between the number of students who are attending camps through GenCyber, which while not the only provider is such camps can be a representative sample of them, and the number of students who are graduating and moving on to college or directly out into the workforce. With that being stated, though, the positive impact of the GenCyber camps shouldn't be overlooked. For 44% of their respondents, a GenCyber camp was the only opportunity they had to learn about cybersecurity (Dark et al., 2021). Additionally, 87% reported that their awareness of the importance of cybersecurity in their everyday lives increased (Dark et al., 2021). So, while only an estimated 1,350 of the graduating high school students are pursuing cybersecurity, many more of them still found usefulness in the material taught.

Preparing Teachers

Another aspect that should be considered is who can teach this content to the students and how they acquire their knowledge on these subjects. At a specialized camp or in an educational setting where there is a formal class, there will be individuals who specialize in or have a field of expertise related to these concepts. However, that can't be stated for every location and is an area that also should be explored. Continued education and bringing the teachers up to date on the issues of cybersecurity and privacy protection practices can help them protect their own information and that of their students and allow them to better relay this information to their students.

Similarly to the students, some initiatives are working to bring continued education or educational resources to teachers to better prepare them to better prepare students. As mentioned previously in the chapter, the Cyber.org initiative of the Cyber Innovation Center is one such program (Cyber, n.d.). This initiative focuses on being able to "empower teachers with resources and training needed to deliver cyber content to students" (Cyber, n.d.). These resources take various forms to provide that help to teachers and reflect several different areas of study. These areas can be related to ethics, liberal arts, or directly to cybersecurity. Some examples are the creation of fictitious scenarios that task students with solving an incident of some type that has occurred (Cyber, n.d.). Using critical thinking, problem-solving, and some cyber skills, the students would be able to make deductions and attempt to find out what happened (Cyber, n.d.).

Other offerings can be more direct continued education, which GenCyber can give another example of with their teacher camps (GenCyber, n.d.). By offering workshops and camps to the teachers, they can grow their knowledge base and build lesson plans around cybersecurity and cyber safety (Dark et al., 2021; GenCyber, n.d.). While this again has many of the same restrictions and concerns that student camps had, bringing more attention to these issues to teachers is a way to encourage them to bring these issues to students. From the GenCyber 5-year report, teachers from the elementary to high school levels who attended the program and participated in the study could teach cyber safety or cybersecurity after attending. Additionally, while the camps themselves cannot always reach large numbers of students for the previously stated reasons, educating teachers can have larger returns over time (Dark et al., 2021).

Active Threats at Southeastern

Data from the Southeastern Louisiana University's Office of Technology can give some insight into current active threats that could be faced by college students (Southeastern Louisiana University Office of Technology [SELUOT], 2019). Through the use of services provided automatically by Google's Gmail as an email service provider and through other in-house means, there are automated measures in place to help prevent phishing or other malicious emails. However, that does not stop user accounts from being breached. The data shows that, while some attachments may be benign, 3,897 attachments were removed from emails. This number does not include messages that were automatically quarantined through Google before reaching the school. Additionally, around 14% of accounts were suspended during the time frame of the data being reported, which accounted for around 22,000 accounts, which is higher than the current semester enrollment because alumni may keep their email after leaving. When some type of suspicious activity or active spamming is detected from an account, it is automatically suspended. Then the user must reset their login information to access the account again (SELUOT, 2019).

These numbers follow a similar path to what can be seen from the yearly threat reports from ENISA and Symantec. In 2018, the percentage of overall email messages that could be classified as spam continued its increase by 55%. This number has been growing steadily since 2015. While the overall number of phishing emails declined slightly, from one in 2,995 emails in 2017 to one in 3,207 in Symantec's 2018 report, the number of emails containing malware remained steady, which was reported at one in 131 emails in the 2017 report. Additionally, out of the malicious attachments reported, 48% of them are from the Microsoft Office suite of file types. These will be files widely used throughout a person's academic and professional career in nearly all fields. Even if a user does not fall victim to a direct malware infection or a directed attempt to gain information from them directly, such as a phishing attempt, there are still many avenues for personal information to be taken without their knowledge (McNulty & Kettani, 2020). One potential technique would be the use of malicious wireless access points that mimic a legitimate access point for a business or other location. For example, at Southeastern Louisiana University, there are 1,244 official Wi-Fi access points. However, there are just as many rogue access points at 1,281. While that does not necessarily mean that those non-official points are malicious, there is an inherent risk if someone was to connect to them versus an official access point (SELUOT, 2019).

Organizations

Another facet that is examined is to look at the organizations that students who are being educated will one day end up joining. Smaller organizations, which are likely to have smaller technical staff just by the merit of their size, are more likely to be targeted by malicious emails (Symantec, 2019a). An organization with 250 employees or less could see as many as one in every 323 emails being of a malicious nature, where a larger organization of 2,501 or more employees may see around one in 556 as malicious (Symantec, 2019a). While it may not be the same across every industry, with industries seeing higher percentages of malware targeted at them than others, it is still highly likely that an employee will come into contact with some type of malicious email, whether that be phishing, spam, or malware, and knowing how to deal with it will lessen the likelihood of data breaches or other problems (McNulty & Kettani, 2020).

Similar statistics can also be seen when looking at the results from the first year of Australia's NDB. This legislation went into effect in April of 2018 and forces organizations covered by it to notify the governing agency and the affected individuals in the event of a data breach (OAIC, 2019). As mentioned previously, from this report on its first year of mandatory participation, an increase of 712% in reports over the previous year when the reporting was voluntary can be seen. Out of the 1,132 notifications, 964 were eligible under the NDB. Of the eligible reports, 60% were attributed to malicious or criminal attacks, 35% were attributed to human error, and only 5% to system faults (OAIC, 2019). In the case of system faults, no direct human intervention caused an error that resulted in a breach. However, in most other data breaches, a human element was involved, with examples of employees sending information to the wrong person or clicking on a malicious link leading to compromised credentials. In what the report terms "Cyber Incident Breaches," the top three types of incidents are, in their listed order, phishing that compromised credentials, compromised or stolen credentials with the method unknown, and brute force attacks compromising credentials. In the cases where the reason was unknown, it was also noted that in many cases, it was from reused and previously leaked information, citing a recent dump of credentials that totaled around 100 billion records. The report also highlighted the need for "sustained and focused user education" regarding recognizing phishing emails along with password management (OAIC, 2019).

Costs of a Breach

When a breach occurs, several cost factors must be considered. There are many different types of costs associated with a breach. However, direct monetary values are easier to see the impact of, as numbers can put to these costs. The Verizon Data Breach Investigations Report notes that 86% of breaches were financially motivated (2020b). High-profile data breaches that affected millions of people at a time can be used as a way of looking at how a single breach can have far-reaching consequences as well as high monetary expenses. The Equifax breach in 2017 not only affected 147 million people but, as of 2019, has cost the company over $1.4 billion (Poyraz et al., 2020). Yahoo! was the victim of the largest data breach, affecting 3 billion user accounts in 2013 and 2014 and a cost of $502 million to the company (Poyraz et al., 2020). While these are the high end of people's effects and costs associated with being breached, it can still be seen that globally, the average total cost of a data breach in 2020 is $3.86 million. However, the United States had a much higher average at $8.64 million (IBM, 2020). Each piece of personally identifiable information was given a value of $150 in the same report, showing the “price” of an individual’s information. The direct costs a business may sustain could include direct financial theft, legal and investigation fees, damage to their stock prices, fines, disruptions to their business, and more (Wang et al., 2019). These affect individuals as well, as it could be their financials being compromised or needing to pay for a service like credit monitoring (Wang et al., 2019).

There are also indirect costs associated with data breaches that businesses and individuals must be concerned with, not just the costs associated directly with the breach. A business may not conduct its normal operations leading to loss of sales, profits, and customers. This can also have a longer-term effect on the confidence in the business that potential consumers or investors have, leading to further losses (Haislip, 2019; Wang et al., 2019). For individuals, the indirect costs of having their information taken when another entity is breach must also be considered. If it is their workplace, they may lose time to earn a wage if the business must stop operations. Still, even if they are only a customer for the business and not an employee, both could experience identity theft, price increases in the services, and damage to their credit (Haislip, 2019; Wang et al., 2019). While these are effects from the breach, the breach itself did not cause the opinion of a company to drop. It was the fact that it happened that did. It was not the breach that directly affected a customer's credit rating, but their information was stolen (Haislip, 2019). There are far-reaching consequences of a breach beyond just the initial loss of data. This can be especially true if a breach is not discovered for some time. In 2020, the average time to identify and deal with a breach was given at 280 days (IBM, 2020). This is when user information is vulnerable, in the hands of malicious actors, and those same users may not yet be notified about the breach occurring.

COVID-19 and Breaches

With the large-scale shift to remote working and schooling environments due to the COVID-19 pandemic in 2020, more people than ever needed to access online resources from home. This included businesses needing to allow their employees access to continue to work from home and students having an increased need to access educational resources over the internet. This had a perceived increase in both the cost and the time it would take to identify a breach (IBM, 2020). This led to data breaches caused directly by the shift to more remote environments (Jayakumar et al., 2020; Verizon, 2020a). As an initial report, from the first of March 2020 to the first of June 2020, 474 data breach records were added to Verizon's repository, with 36 of them being directly attributed to the COVID-19 pandemic operational shifts (Verizon, 2020a). With attacks on web applications more than doubling from the previous year, it can be expected that as more time passes and more incidents are reported on, that further attributions will be made (Ahmad, 2020; Mandal & Khan, 2020; Verizon, 2020b). Additionally, with more than a quarter of all breaches being attributed to human error and with a large number of breaches caused by stolen or brute-forced credentials, this trend can be expected to continue (Mandal & Khan, 2020; Verizon, 2020b).

Similar Studies

As far as actual knowledge studies go, there are not many questions and answer sets available to help gauge what has been done. A familiarity survey was performed by Alexis Neigel et al. to attempt to solicit information from college students on a five-point Likert scale with their familiarity with "cyber hygiene" concepts (Neigel et al., 2020). While this cyber hygiene study was performed on a similar group of University students, the metrics and exact information being measured were different. Additionally, there is a study that was conducted by the Pew Research Center that performed a similar study to this research in that their study asked direct questions to their participants. However, their survey population was a very wide group of individuals (Olmstead & Smith, 2017).

The cyber hygiene study looked at 173 undergraduate students after cleaning their data and used several measurements to determine behavioral patterns. In their paper, it is stated that "participants indicated that they were both highly aware of and actively engaged in several factors related to cyber hygiene" (Neigel et al., 2020). The related areas mentioned included password management, use of email, surrounding awareness, mobile device and Wi-Fi use, and social media postings, among others (Neigel et al., 2020). This does fit in line with the general areas that this survey also covers to an extent. However, awareness of cybersecurity and privacy protection issues and understanding and implementing proper practices are not necessarily equivalent. Their study looking at the human factors and behavior is very much an important piece in determining how best to educate individuals, but could be coupled with concrete examples to assist in determining actual understanding.

The report by the Pew Research Center has the most applicable research (Olmstead & Smith, 2017). Their report asked 1,055 adult internet users in the United States a series of thirteen questions that aimed to identify some cybersecurity knowledge by using a series of multiple-choice or picture answer questions. While their survey group is broader than the group studied for this research, the results can help shed some light on existing ideas and form a basis on which this research survey can build. For example, in their survey, they offered the survey takers a choice of four passwords and asked them to choose the strongest password from them. A majority could do this, with only 25% being unsure or incorrect in their response. Of the responses, 54% were able to identify a phishing attack from a set of descriptions. However, as they moved into questions such as what HTTPS in a website's URL meant, more individuals became unsure or incorrect. For the HTTPS question, only 33% were correct while 54% were unsure what it means, 70% of respondents were unsure of the use case for a VPN on an insecure Wi-Fi network, and 71% were incorrect identification of a multi-factor authentication screen image. These questions can begin to give us an understanding of where their population's knowledge level was. Additionally, the Pew survey broke their results into education and age ranges for the number of questions answered correctly. By examining those who have an education of high school or less, they answered a mean of four questions correctly, and those with some college education answered with a mean of 5.5 questions correct. With the age range of 18-29, which is where many of the standard students for this paper fell, the mean number of questions answered correctly was six. This can tell us, again, that there is a wide range of knowledge, but also that there is a large knowledge gap in this population. Their population skewed more to the higher age ranges, with only 175 of their 1,055-sample size being in the 18-29 user range (Olmstead & Smith, 2017).

Chapter Summary

By looking at what is currently being done, it can be seen that there is a lot of effort going toward cybersecurity education. However, the recipients of this education and the knowledge they receive can vary widely. For those in a technical major, there can be one or more accrediting bodies that help ensure the correct material is covered to specified levels of rigor for the program the student is in, assuming it is accredited. Many, however, will not fall into these areas of study. As has been shown, that doesn't mean that they will have any less of a need to know the basics of cybersecurity to protect themselves and their data, but it does mean that they might not be receiving the information directly. They would be required to seek the knowledge themselves, but this will come at the cost of time or money that could be spent elsewhere, leading to a lessened desire or ability to educate themselves. However, the costs associated with having their private information leaked, even if they are indirectly linked to the breach that leaks it, still apply. Additionally, few studies are being done in the area of educating the general public. Where studies are being done, the population is either very wide or has focused on individuals who are already practicing good habits. In the next chapter, the research methods associated with this study will be discussed in more depth, and then in the following chapters, the results of the survey will be presented along with the conclusions drawn from it.

CHAPTER 3

RESEARCH METHODS

The purpose of this study was to examine several key areas of cybersecurity and privacy best practices and seeks to gauge a generalized knowledge level of college students at Southeastern Louisiana University, to assess how well these areas are understood, and to see if there are any misunderstanding among what is believed to be known. The study was designed to gain a greater understanding of areas within the cybersecurity realm that these students who may not be exposed to basic principles depending on their background and chosen major understand, where they lack in understanding, and where they may have misconceptions on the various topics. This study expected that it would show areas where students have ranging levels of competency in the basic principles of cybersecurity and privacy protection and associated technologies. This chapter will explore the approaches taken in the design of the research, the reasons behind choices made during it, the creation of the survey instrument, and its validity.

Research Design

There is research that studies how a student pursuing an education in cybersecurity is taught the deeper concepts of the discipline (ABET, n.d.; NSA, n.d.). There are also frameworks in place that can be used to create an education program for these types of students. The National Security Agency's Centers of Academic Excellence is one such example. An institution may be certified as a Center of Academic Excellence with one or more of three cybersecurity designations, Cyber Research, Cyber Defense, and Cyber Operations (NSA, n.d).

Each of these designations holds a standard that the institution must meet to be certified as one of these Centers, which allows for a certain rigor in the discipline. However, there is no standardized way in which students who are not pursuing a degree in a related field may obtain an education in the basic principles used by nearly every individual today.

In many education programs, there are no such courses that a student may take, let alone be required to take, to allow a student in another major to receive information that is increasingly vital for use in not only their future jobs but also their everyday lives (Dreibelbis, 2016). There is some research taking place on beginning some education in high school or before. However, this occurs in very few locations (Pye, 2016; Scheponik, 2016; Schwartz, 2018; Skinner, 2017). Additionally, this would be too late for many students who have already graduated from high school and have entered college or who are not seeking further education at all.

Research Method

This study employed a quantitative survey method as defined by Creswell (2014) to give numeric values to the responses given by individuals. The survey can be used to form a generalized, quantifiable understanding of the knowledge base of the study's population. The goal of a survey design is to provide a "quantitative or numeric description of trends, attitudes, or opinions of a population by studying a sample of that population" (Creswell, 2014). This fits in line with selecting a portion of the student body to survey, which is discussed later in this chapter. Using an online survey to collect the desired data from the students is the strongest candidate for usage in this study. The reasoning behind this choice is that it provides several key benefits for both the participants and the researcher. The benefits to the participants are that a well-known name can be associated with collecting their data, and while no identifying data would be collected for the study, having the confidence that comes with a familiar platform was seen as a positive to the researcher. It would also allow them to take the survey when they were able, and on whatever device they would choose to use as a large survey platform would accommodate a myriad of devices. For the researcher, it allowed for greater ease in collecting data, with a single survey link being used for all participants and all responses being gathered in a single place. Additionally, the platform allowed for additional screening of participants to ensure they fell within the sampled population.

Data Collection Tool

This study used a web-based surveying tool to facilitate students' ease of use and gather their responses. The survey was used to assess the knowledge areas that are the focus of the study. Since the target population are students within many different degree programs and not students within cybersecurity, computer science, or other related programs, the survey mainly assesses basic concepts and surface-level ideas that are common occurrences for most individuals. Based on the survey results, competency levels in these basic areas were assessed, and then from these competency levels, recommendations for potential solutions are offered.

Survey Population

The population that was used for the survey is students at Southeastern Louisiana University. Southeastern Louisiana University has an average student population reported at 14,371 for the 2016-2020 period and the Fall 2020 population given at 14,461 students enrolled

(Southeastern Louisiana University Office of Institutional Research [SELUOIR], 2020c; SELUOIR, 2020b).

By looking at students from as many disciplines as possible and all levels of study, a larger cross-section of students could be observed. It could also be observed if there are any correlations between where a student is in their academic career, or their chosen major has an effect on their knowledge levels that were evaluated. This also ensured that as many students, majors, and backgrounds as possible are reached.

The limitation of surveying students at a single university is that many come from a small number of places, which can impart an inherent bias to the results. However, it may still be generalized to the local population at the university. With the population of 14,461 during the semester of the survey being administered, based on formulas from prior research, a sample population of 385 would provide a statistical significance with a confidence level of 95% and a margin of error of 5% (Cochran, 1977; Barlett et al., 2001; Israel, 1992). This value was obtained using Cochran's formula with a t-value of 1.96 to provide the 95% accuracy level and a value for d given as .05 to account for the 5% margin of error. Additionally, since the survey would be looking for either right or wrong, no matter the form the question took, and there was no assumption made that students would have an equal opportunity to answer right or wrong, a p and q value of .5 was used for each. This allows the survey to be generalized to the university population with an expected high degree of accuracy.

Survey Participation

The Office of Institutional Research selected a random sampling of students at Southeastern Louisiana University, and their university email was provided to facilitate contact. These randomly selected students were contacted via their university email to solicit their participation in the survey. The initial email to the potential participants contained information about the principal researcher and the survey, the length of time it was estimated to take, a statement about it being voluntary, and a link to the survey. This would ensure that before accessing the survey, the individual would be aware of the fact that the principal researcher held a faculty position at their current university while being a student at a different university and that there was no requirement for them to participate nor a reflection of participation within their academics at all.

Within the survey, before an individual could participate, they were given more detailed information about the survey, their rights as a participant, additional information on how to contact the researchers, and how they could contact the Institutional Review Boards at Southeastern Louisiana University and Dakota State University. These statements and information provided a full informed consent to participate in the survey if the individual chose to. Additionally, only individuals who were older than 18 years of age were eligible to provide their informed consent.

While the random sampling should not have included any individual under 18 years old due to how the Office of Institutional Research performed the selection before the full survey began, the participant's age was asked. If they answered that they were under 18, then the survey would thank them but would filter them so that additional questions were not asked. Other age groups that were eligible to participate would be sent into the full survey.

Survey Research and Design

Survey research "provides a quantitative or numeric description of trends, attitudes, or opinions of a population by studying a sample of that population" (Creswell, 2014). This survey research can be broken into three main areas: the survey of knowledge, the assessment of the knowledge areas and interpretation of data, and the recommendations that can be made from the assessment. While these are all distinct steps, they are not independent and rely on the previous step before the following can begin.

The survey design is based on the survey presented by Olmstead and Smith (2017) from the Pew Research Center. Their survey covers some of the ideas that this survey wants to present. However, several questions are outside of the scope of this research. Additionally, their survey had a much broader target population than this research is attempted to assess. However, using their survey as a base, then a preliminary usage of many of the question ideas had already taken place. There were changes made for this survey in both removing and adding questions to make it better fit the intention and goal of the research. These changes and the new survey were reviewed and validated by a specific committee and some volunteers who hold positions in computer science, cybersecurity, and education fields. This was to ensure that the questions in the survey correctly addressed core issues desired and did not contain information that was overly technical in most cases.

As noted previously, this research survey's goal is to assess the level of basic cybersecurity and privacy protection knowledge among college students. These goals mean that the survey needed to be as non-technical and clear as possible. The correct meaning and intention of each question are understandable by everyone, with no special knowledge needed. However, ideas that individuals come into contact with every day, even if they lean more toward the technical side, are considered acceptable for the survey. For example, an area assessed is related to passwords in both this research and the Pew Research survey. Another topic that is assessed by both is the difference between HTTP and HTTPS. While the exact implementation of HTTP versus HTTPS would be too technical for this study, the difference between them is something that individuals should know and look for when browsing the internet.

Chapter Summary

The purpose of the study was to explore knowledge areas and common technologies in the general cybersecurity and privacy protection realm in which students at Southeastern Louisiana University show proficiency, misunderstandings, or deficiency. The reasons behind the methodology used in this study were given and the choice of a type of survey platform. Information over the population and participants in the survey was also provided, and the design decisions for the survey itself. In the following chapters, the results of the survey will be provided in detail, and recommendations will be made with the intention that in the future, they may be used to help improve the level of proficiency in these basic cybersecurity and privacy protection knowledge for students at Southeastern Louisiana University.

CHAPTER 4

FINDINGS AND DISCUSSION

This quantitative research studies the general knowledge level of college students at the Southeastern Louisiana University on topics related to cybersecurity and privacy. With a survey being performed over a portion of the student population, a gauge of the base-level understanding that the participants can be gained for the assessed areas. This can then be used to identify areas of weakness in current knowledge areas.

This survey research provided an accurate representation of where the student population understands the subject area well, where they do not understand the subject, and, perhaps as importantly, where there are misconceptions in the areas presented to them. These three types of responses are just as important as each other in determining how the student population treats and understands the subject areas. The complete survey can be found in Appendix A.

In this chapter, the research information, population, and method will be presented. Initially, information on the participants and the structure of the survey is presented. The findings of the survey will then be presented. This chapter will then end with a discussion of the findings.

Methods

Research Approval. Due to the survey including students as the target participants in the survey, IRB approval was required. Since the student population being surveyed would be at another university, Dakota State University IRB requested that the Southeastern Louisiana

University IRB issue approval first before being reviewed. Southeastern Louisiana University IRB approved the survey, and it was then sent to the Dakota State University IRB, where it was also approved. All students would be eligible to participate as long as they were eighteen years or older.

Research Population. The IRB-approved survey was sent to a random sampling of students whose university email was provided by the Southeastern Louisiana University IRB. The provided emails were from students in all majors, classifications, and standings present at the university in the Fall of 2020. The email group did not encompass the entire student population. However, the student email addresses of five thousand students were given to be emailed the survey.

Students as of Fall 2020

- 14,461 students enrolled
- 13,490 undergraduate students
- 971 graduate students
- 64.1% female
- 35.9% male

Academics as of Fall 2020

- 5 academic colleges
- 21 departments
- 43 undergraduate degree programs
- 20 master's degree programs
- 2 doctoral programs
- 4 100% online programs
- 2 100% online Post-Masters Certificate Programs

Table 1 – Southeastern Louisiana University Students and Academics

From Southeastern Louisiana University's Office of Institutional Research, the university's relevant student population, demographics, and major information are given in Table 1 (SELUOIR, 2020b).

These numbers will be considered when looking at the individuals who responded to the survey and the demographic information obtained. However, it should be noted that the count given is of degree programs within the university does not consider each major within the programs individually nor more specialized concentrations or other degree programs that could be offered. For example, within the Computer Science department, there is a Bachelor of Science in Computer Science and a Bachelor of Science in Information Technology seen as two degrees. However, within the Computer Science degree, there are three concentrations that each require different curriculums, a Scientific concentration, a Data Science concentration, and a Pre-MBA concentration. This will cause inflation in the number of degree programs being sought by students, as reported by themselves in the survey, later in this section.

Research Execution. Google Forms was used as the online survey platform. This allowed for easy solicitation of the students by linking to a well-known company when contacted through email. This also allowed for easy screening of the participants and their answers by only allowing them to continue to the research question after reviewing the necessary IRB information and confirming that they are eighteen years of age or older.

Of the solicited student participants, 811 responses were received, of which 810 were able to complete the survey. The one response that was not eligible to complete the survey answered that they were under eighteen, and the survey design then did not allow them to complete any of the research questions. With that, all participant responses to the research questions are valid responses and fall within the IRB approval of the survey's desired population.

As mentioned in the previous section, to obtain a 95% confidence level with a 5% margin of error, 385 results were needed. With a total of 810 usable results, this goal was met and surpassed. So, recalculating with a 99% confidence level and 5% margin of error, then the number of responses needed becomes 664, which is still less than obtained. From the previous formula given, the only change made was to the t-value, which was changed from 1.96 to 2.576.

Survey Demographics

Research Participant's Ages. As stated previously, the age range for the survey was eighteen years or older. With the additional idea that the survey population was college-age students, a non-linear scale for age was used. More stereotypical college ages were grouped in smaller ranges, expanding as they increased, as seen in Figure 1.

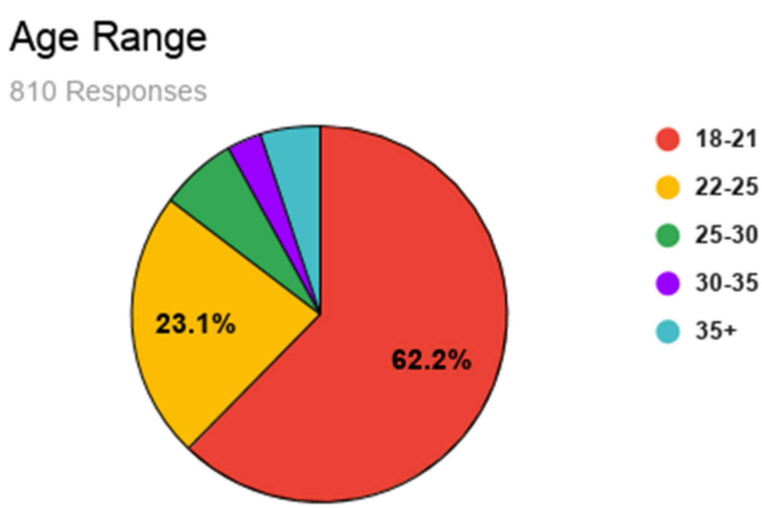

Figure 1 – Participant Age Range

A majority of participants fell into the range of 18 to 25 years of age. This was expected as that is the typical college student age range, and these values fell in line with reported statistics by the University (SELUOIR, 2019). Just under 15% of the responses fell outside of this range. With 6.7% falling between 25 and 30, 3% falling between 30 and 35, and 5.1% answering they were older than 35. This set of responses allows for the focus to remain on the younger college-age students while still providing some information about those who have returned to college, started later, or stayed longer. While the exact population values are not yet published for the Fall semester of 2020, the ages and genders of students can be seen not to have a wide variance of change between 2015 and 2019. A chart containing the ages and genders for the University can be found in Appendix B (SELUOIR, 2019). All further demographic and major information must be considered because no student under the age of 18 is represented.

Research Participant's Gender. While not expected to be relevant in determining knowledge levels, the participant's gender was asked, though not required to be given. This was to give a better understanding of the population that had completed the survey regarding the university population.

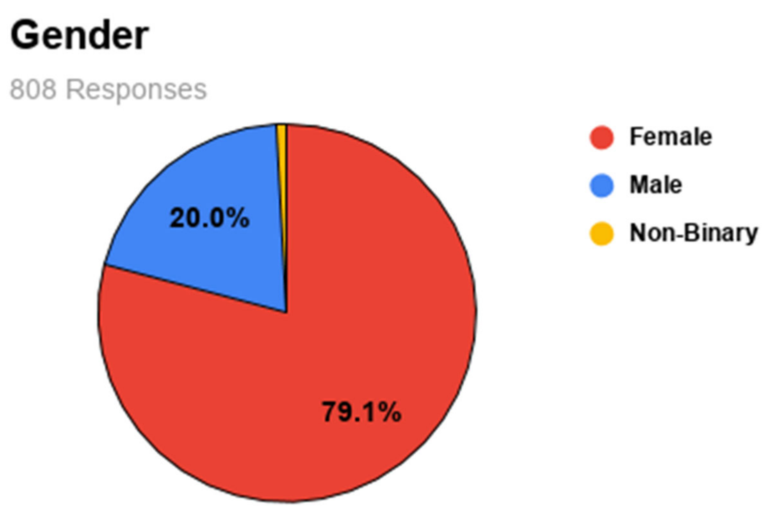

Figure 2 – Participant Gender

As previously stated, the participant's gender was not required to be answered in taking the survey. However, only two individuals opted out of answering the question, as shown in the response count of figure 2. While there appears to be a large skew toward female responses, as shown in the previous chapter Southeastern Louisiana University has a much larger female student population than the male population, with the university being at 64.1% female and 35.9% male (SELUOIR, 2020b). See Appendix B for a breakdown of past University values for gender and age (SELUOIR, 2019).

While the percentage of female participants is higher than the university, this can be attributed to the random sampling of students, the majors of the participants, and the ability to self-identify. With the latter of those in mind, 0.9% of those that responded identified as a Non-Binary gender.

Research Participant's Classifications. The academic classification of the participants was also requested. Of the responses, there was no overwhelming majority, as seen in other demographic information. This leads to a fair split among all academic standing, except graduate students, which were expected to be lower than the others by the number of students enrolled as graduate students in the fall of 2020, as previously shown.

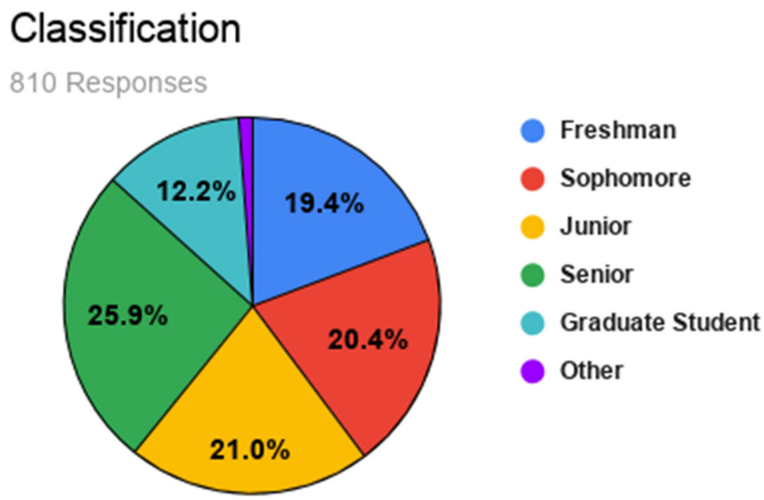

Figure 3 – Participant Academic Standing

In figure 3, the percentage breakdown of each category is shown. There is a slight leaning toward those of Senior standing, but not significantly enough to have an expected effect on the other gathered data. The Other category was provided for those that did not fit well within the traditional classifications. This selection made up only 1.1% of the responses and included individuals who identified themselves as earning certificates, returning for a second degree, or were transfer students who had some technicalities in their standing.

Research Participant's Major. Participants were asked to provide their current major. This allowed for the individual's chosen major to potentially be included as a factor for some participants being more likely to come into contact with the concepts presented than others. As mentioned previously, the university report does not consider concentrations or more specialized versions of the various degrees even when the curriculum for them differs. This leads to a seemingly inflated number of majors when self-reported on the survey. Additionally, with the self-reporting nature of asking the student, they may consider their major to be something other than its official name, which further increases the number of reported majors.

Overall, 107 different majors were reported by participants in the survey. Many of these being a more specific version of some study areas, such as separating Math Education or Music Education, etc., from simply Education. Additionally, many student's stated majors did not fit in line with one reported by the University. This was an unforeseen issue that solutions will be discussed in a later section. A listing of degrees offered by the University and their populations for the Fall of 2020 can be found in Appendix C.

Within the majors reported, many only included single individuals. However, several majors had more individual responses than others. Nursing has 107 individuals responding to the survey, Psychology had 55, Kinesiology had 44, Accounting had 34, Biology has 32, Criminal Justice had 28, Business Administration had 27, Computer Science had 25, General Studies had 23, and Social Work had 19. These were the top ten responses to the survey in the number of participants per major, though there are still other majors with five, ten, or fifteen to eighteen responses from them. A complete listing of all reported majors on the survey and their counts can be found in Appendix D.

When comparing the majors that produced the most respondents with the enrollment numbers that the University gives, several of the same top listings can be found (SELUOIR, 2020a). From those statistics, the Undecided major is the largest anomaly to note. It represents the top number of majors reported by the University while only being represented by a single individual in the survey. The best conclusion for this anomaly is that since the survey does not have any participants under the age of 18, that a majority of those that are Undecided fall into this age category. As a student progresses, they choose their major. While speculation, it would fit in line with general expectations placed on students. The majority of reported Undecided students are also part-time students, which could inflate the number by adding those who do not intend to fully commit to a major specifically at this University (SELUOIR, 2020c). Additionally, the random nature of the sampling of students could simply have missed any older Undecided students. For other majors, Nursing takes the top spot by a large margin as reported by both the University and as seen in the survey, with most other majors falling in similar positions numerically as seen in the survey, even if not in the same order.

Findings

Survey Results. In this section, the survey results will be presented and looked at independently of each other and demographics. The survey questions will not be presented here in the order that they were asked in the survey. Instead, it will be shown to increase apparent difficulty based on participant responses. Each question's results will be presented as a figure and then discussed immediately following.

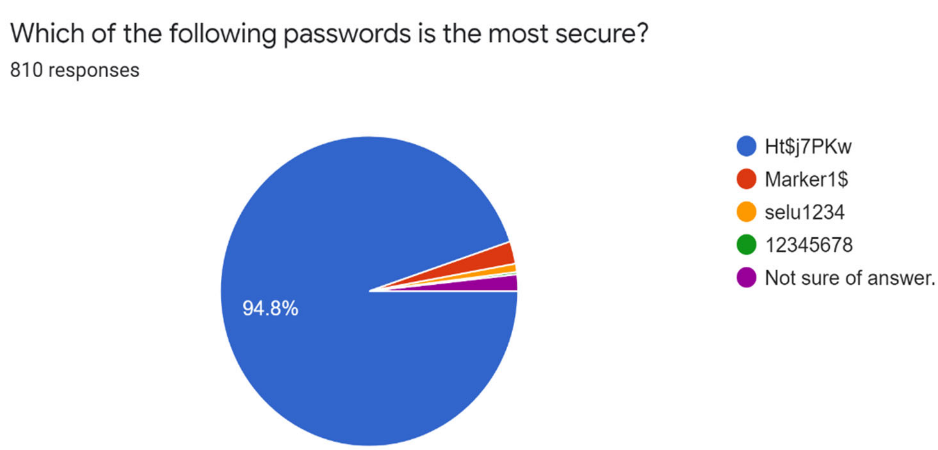

Figure 4 – Survey Question Eight Results

In figure 4, a question that presented a simple set of passwords to the survey participants is shown to gauge understanding of password strength. While none of the presented passwords are considered secure, they were to identify which one would be the most secure of the given options. All passwords given were the same length to avoid as much ambiguity as possible in the answers provided. As seen in figure 4, most responses selected the password created from randomized letters of multiple cases and contained a symbol and number. This was the expected result as a typical password policy will encourage a user to use a similar password, as does much of the available information. With the wide usage of passwords for everyone, being exposed to the best practices for a password is highly likely. However, even with this in mind, a small percentage of the responses either chose an incorrect option or were unsure of the correct answer. Ensuring that individuals understand the reason behind why a password policy asks for certain restrictions on passwords to be followed would likely help individuals be more confident in choosing strong passwords.

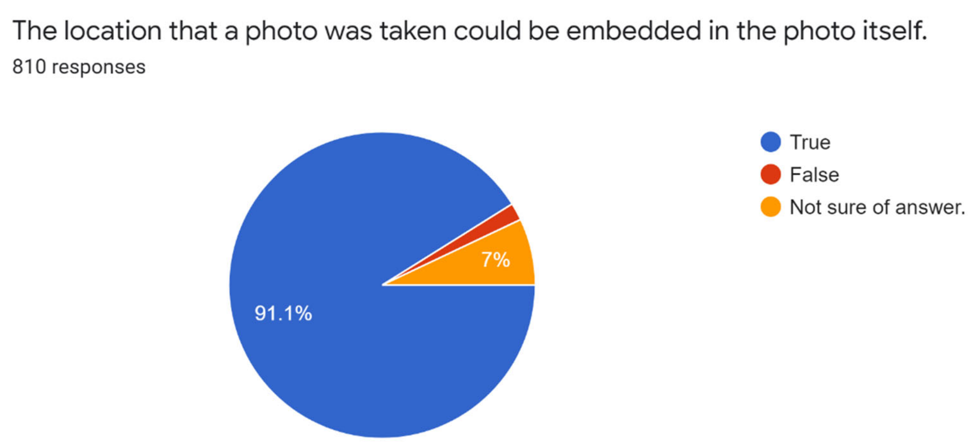

Figure 5 – Survey Question Ten Results

For the question presented in figure 5, the idea of location privacy was addressed in terms of what could potentially be embedded in the photograph's format, not necessarily incidental location leaking by what is in the picture's contents. Once again, in this question, most of the responses correctly identified that this was a possibility. While not completely so, it has become more common knowledge that photographs can contain GPS data or other identifying information embedded in them, especially with the continued growth in smart devices as cameras. A portion of the responses was unsure about this topic or incorrectly stated that the location could not be embedded in it. Making it clearer what is being saved in the formatting of photos being taken and having a clearer path to choose would likely help make sure everyone can decide on this topic. While not the sole reason that location information could be leaked or private data exposed in this manner, the fact that most participants were aware of the possibility of this type of information exposure is positive.

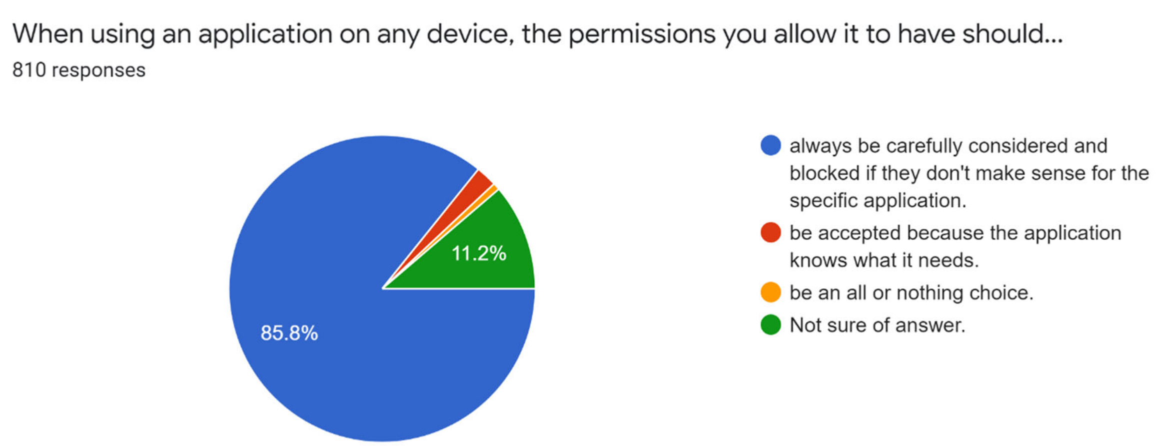

Figure 6 – Survey Question Eleven Results

This question asked participants to complete a thought regarding the permissions given to applications and intended to have the participant think about some application they have placed on their smart device, laptop, computer, or similar devices that asked for permission to use one of its various functions. While still an overwhelmingly correct response in that the permissions are given should be carefully considered, a decent number of individuals were not sure how they should treat it. With the growing number of malware applications on legitimate stores for smart devices of all brands, as mentioned previously, the importance of understanding when to accept or deny permissions for applications is also growing. Thinking critically about why an application may need access to a certain service or functionality can greatly reduce the risk of a rogue application getting access to information that the individual may not wish to share. Having developers show why their application is asking for permission to use a device resource could assist in this. However, in the end, it will still fall to the users to understand the risks associated with allowing access to various resources and determine if they make sense on an application-by-application basis.

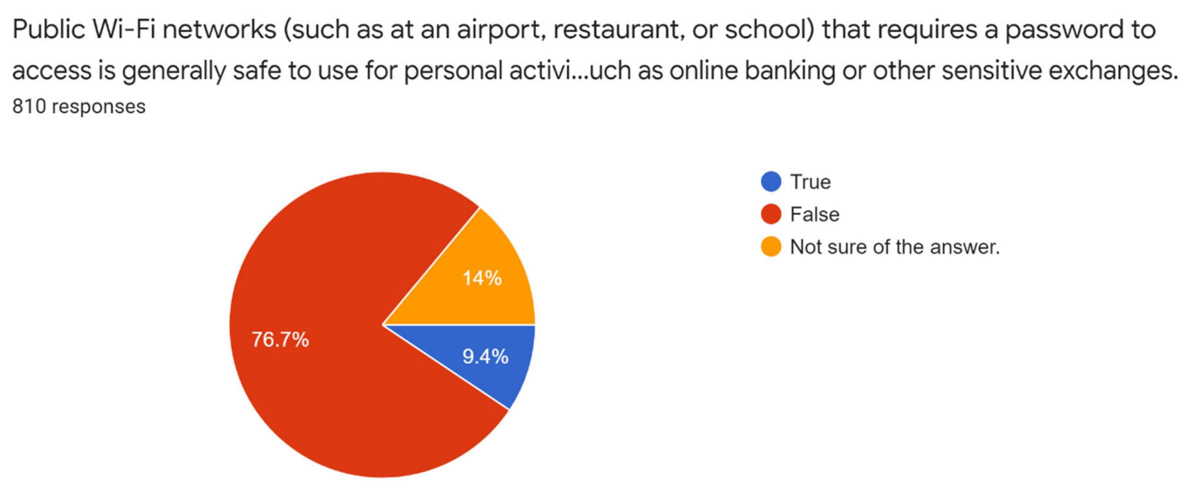

Figure 7 – Survey Question Thirteen Results

For the question depicted in figure 7, participants were asked whether publicly accessible Wi-Fi networks were safe to use for personal exchanges or viewing sensitive accounts such as credit cards or online banking applications or sites. Just over three-quarters of the responses did believe that this was not the case. Since an individual cannot be sure who is also acting on these networks, precautions should always be taken, and as such, it cannot be said that they are completely safe. With the abundance of these types of networks that can be seen in restaurants, businesses, workplaces, schools, and other locations, the importance of understanding the risks of using them should be well understood. Many require simple passwords, can be used by any patron or former patron depending on when or if the password is changed, and can potentially be accessed from outside the building, giving malicious individuals ample opportunities to do whatever they will with the legitimate access point. Some individuals are unsure of how safe that these access points are or are trusting in them. While giving some trust may be okay depending on the exact circumstances, being skeptical would likely be a better approach. At the very least, knowing that something could potentially happen would be helpful knowledge for all.

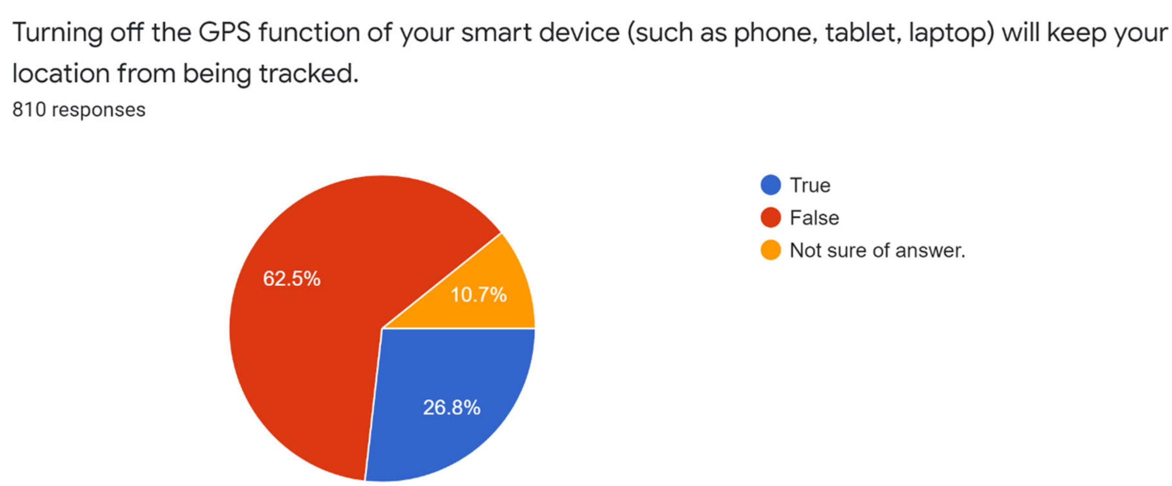

Figure 8 – Survey Question Nine Results

In survey question nine, the topic returns to the idea of location tracking. However, in this case, it deals with the GPS function present on many smart devices and whether simply turning it off is enough to keep your location from being tracked. There is a myriad of ways that location can be determined, either roughly or precisely, such as internet connection location, cell phone towers that you are connected or connecting to, analyzing information that is being shared via social media, or many others that do not require any physical contact with the individual. This can be seen when connecting to location-based services such as whether that can if they do not have access to your GPS data, guess your location based on IP address. This guess may not always be accurate, but it does demonstrate the point. In this question, it can be seen that a majority are aware that simply stopping the GPS function of their device is not enough. However, a sizable portion believes that it is, and then others are also unsure whether this is true or not. If an individual was being stalked or tracked through the usage of means other than GPS, knowing what could be giving away their information beyond simply telling someone or making use of GPS data could help them.

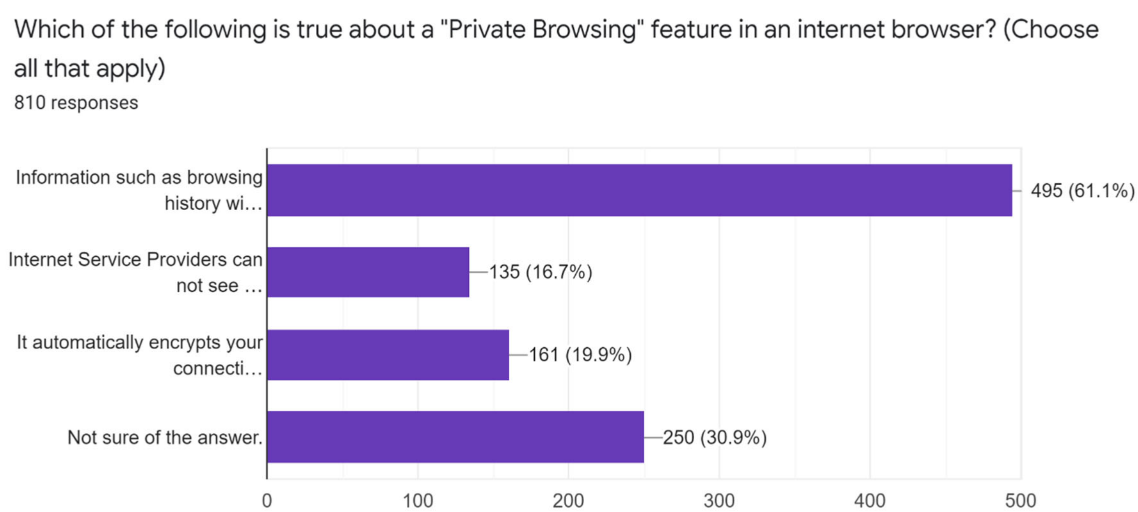

Figure 9 – Survey Question Six Results

A common feature in most modern browsers is a private browsing mode. It may be called different things based on the browser, but the main idea behind them is that certain browser functionality may be altered, and certain information not retained or sent as normal. In question six of the survey, individuals were asked to choose from a list of what they believed that this browsing mode did. One of the most common features of private browsing modes is that any internet history of sites visited while active will not be retained. While most participants selected that their browsing history would not be kept after the session, many chose multiple responses meaning that there are conflated ideas about what this mode does. Of the responses, 328 chose only the response about browsing history. This means that the additional 167 responses to that choice included other options as well. Additionally, many participants indicated that they were not sure of the answer when selecting other options giving further confirmation that this mode is not as well understood as it should be while being used and could be giving individuals a false sense of security in certain actions that simply is not the case.

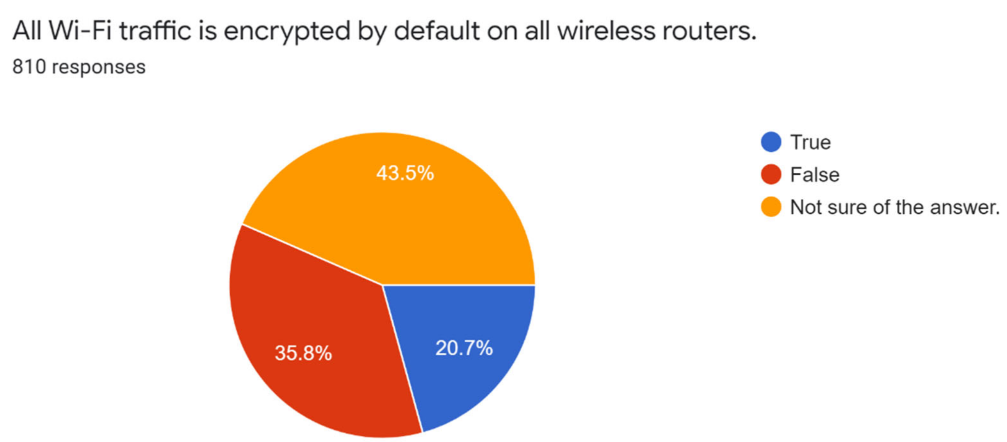

Figure 10 – Survey Question Twelve Results

Figure 10 shows survey question twelve, which asked the participants whether Wi-Fi traffic was encrypted when they used a wireless router. For this question, a larger portion of the respondents was unsure of the correct answer, and a significant portion mistakenly believed that this was true. While it is possible that traffic could be encrypted, the assumption cannot be made that it is without looking into it for a given access point. This means that most of the survey participants could be unwillingly putting their data at risk by either mistakenly assuming that they are safe or by not being fully aware of what to look for to see if a connection is encrypted. This could be especially true with mobile applications where it is not always clear whether the connection it is using is encrypted. More on this topic will be discussed when looking at question seven of the survey.

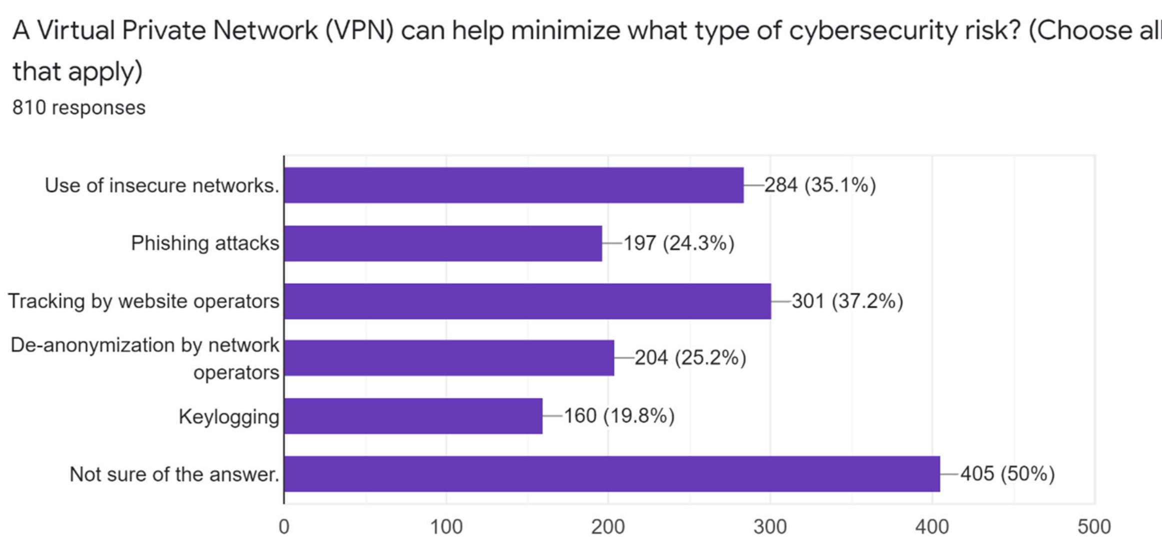

Figure 11 – Survey Question Fourteen Results

Figure 11 illustrates the responses given by survey participants to their knowledge of how a Virtual Private Network (VPN) helps protect them. Of the choices given, any number could be chosen. However, the only one that is a real benefit from the above choices is the use of insecure networks. The other options are either unrelated completely to using a VPN, such as phishing attacks or keylogging, or they can still be accomplished even if a VPN is being used. Of the 284 responses that correctly chose insecure networks, only 37 chose that response solely. To contrast this, of the 405 that stated they were not sure of the answer, a total of 372 chose that response solely, and only four individuals selected every option. This means that under 5% of participants correctly identified the usage of a VPN on the survey for the given options. While the exact knowledge of how a VPN works is not something that would be considered common knowledge, the use cases for one and how they can help should be as more individuals begin to use a VPN.

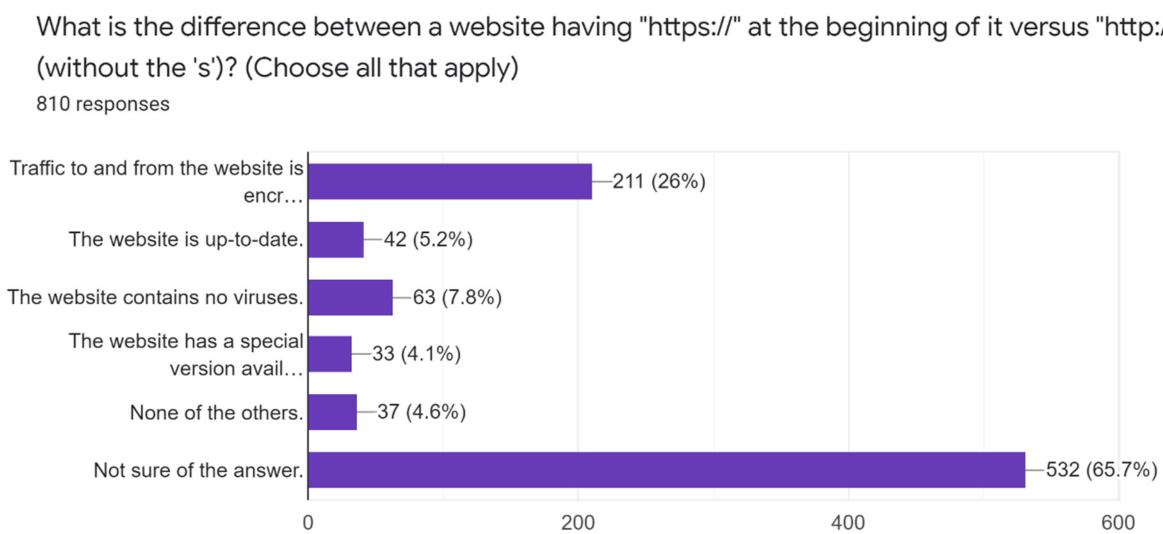

Figure 12 – Survey Question Seven Results

Question seven, as seen in figure 12, returns to the idea of secure connections. In this question, it is asked, non-technically, what the difference between a website having HTTPS in its address versus just HTTP. Of the choices provided, participants were allowed to choose as many responses as they wanted for this question, with the correct response being that the traffic to and from the website is encrypted. A clear majority here were unsure of the difference, with 507 of the 532 participants who selected only that response. Of the 211 that did choose the correct response, 144 chose only that answer, and another 11 chose that plus that they were not sure. The responses here, along with those from question twelve above, show that many individuals do not know when their connection to a website is secure or not. This can lead to sending private or sensitive information over unsecured connections allowing breaches of privacy or accounts to happen more easily.

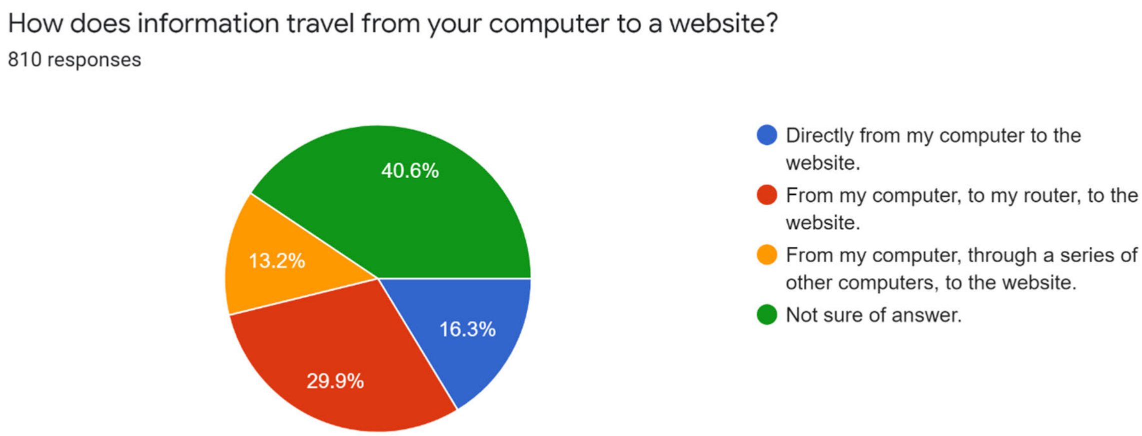

Figure 13 – Survey Question Five Results

In figure 13, the results for question five are presented. At a very shallow level, this question asked participants how information travels over the internet with the intent to see if the general idea of how the internet worked was ubiquitous. Unfortunately, only 13.2% of the participants gave the generalized answer that the information would travel through a series of other computers between them and their destination. Of the rest, 40.6% were unsure, and 46.2% chose incorrect answers. This lack of basic understanding of the basic functionality of the internet, while not being unexpected, was at a larger amount than anticipated. There is likely a link between the responses seen to this question and the seeming disconnect between how many cybersecurity and privacy issues are perceived and handled.

Survey Results by Demographics. In the following sections, the demographic information obtained in the survey is applied to the results from the individual questions. This enables the ability to see if a participant's age, how long they have been in school, as referenced by their academic standing, or majorly affected their responses. Not all majors will be examined, only the top ten by response rate.

Overall Results by Age. The participants' age was considered one potential factor in determining how familiar with the concepts and ideas presented in the survey an individual was. However, upon examination, age was found to not play a statistically significant role in the answers provided to most questions. While there may have been some slight variance in exact percentages, most age groups answered questions in the same manner as each other, except for one question. The question that showed some deviation between different age groups was survey question five, which asked how information traveled from their computer to a website. No age group presented a correct response rate that met their average response rate. However, the 25-30 age was more apt to answer that they were unsure of the answer compared to the incorrect options, and the 22-25 and 35+ age ranges gave more incorrect responses than their other response rates. In the other age groups, the incorrect and unsure response rates were near equal. Overall, it does not age did not appear to play a factor in the responses given by the survey participants, and when there was a slight variation, there are other factors that could have caused it rather than age.

Overall Results by Classification. How long an individual has been advancing in their studies was another demographic collected to be examined. This was accomplished by looking at their academic standing with the assumption that a freshman would have been, on average, in college for less time than a sophomore, who would have been there for less time than a junior, and so on. This would also mean that they would have taken more classes toward completing their degree. While this is generally heavily tied to an individual's age, there were Freshmen of ages in the 18-30 ranges and higher classmen from all age groups. As expected, the higher the classification, the more the upper age ranges are represented. However, they are all still college students, no matter their age.

As with the age of participants, their classification did not show any significance regarding their responses to most questions. There was one question that had a higher degree of variance than others. That question was survey question number twelve, which asked whether Wi-Fi traffic was encrypted by default on all wireless routers. Participants that were freshmen or sophomores, compared to their average response rates, showed that they were more likely to state that they were unsure of the answer. The significance here is that their average incorrect response rate was that different from the other classifications, but instead, their correct response rate was lower. While the higher classifications averaged around the same number of correct versus unsure responses, freshman and sophomores averaged higher unsure responses and lower correct responses. This also showed that junior, senior, and graduate students had an average correct response rate to this question, and that number was nearly identical to the number that stated that they were unsure of the answer. This was the only question that showed a significant difference for any individual group compared to the overall result. So, while overall, there was no significant change to any result by looking at the academic classification of a participant, the one discussed question did have a slight change to its result.

Overall Results by Major. Since many majors did not have a significant number of responses attributed to them, only the top ten majors by response rate were examined versus responses. These majors were Accounting, Biology, Business Administration, Computer Science, Criminal Justice, General Studies, Kinesiology, Nursing, Psychology, and Social Work. While there is a shared general requirement for certain classes that are university-wide, each major will have its own unique set of course work that must be completed for a student to earn their degree. This means that each major is going to expose its students to information on different topics. With this in mind, a student's major has the potential to be the biggest swaying factor when it comes to them being exposed more readily to the concepts and ideas presented in the survey. More computer and technically focused majors are potentially more likely to contact these concepts or have been taught them directly.

The Nursing major has a significantly larger total population than the other majors listed. This is due to the random nature in which the participants were selected and the size of the nursing program at Southeastern Louisiana University. However, only in the freshmen classification does it have a substantial lead over the other majors. While it retains the greatest number of students in each classification, it does not have as overwhelming a numeric lead in the others. See Appendix E for a breakdown of how many participants from each major were represented from each academic classification. As in the other section, since there is not an equal number of students in each major, the average response number per major will be used to mitigate the fact that there was a large numeric difference in the number of students in each major.

As with the other demographics, the responses given to the survey questions by the top ten majors were compared to each other and the overall result from each question. However, unlike the other demographics, one major had consistently equivalent or higher correct response rates than the other majors comparatively on all questions. That major was Computer Science. While there were still individuals who were unsure or got the questions incorrect, there was a significantly higher percentage of computer science participants that did answer the question correctly when compared to the overall responses and other majors. As an example, from survey question twelve, as was seen in figure 10, only 35.8% of all participants selected the correct response. However, when isolated, participants in the computer science major had a correct response rate of 60% to this question. This trend followed for most questions, with computer science meeting or exceeding the overall correct response rate. There are still obvious misconceptions that can be seen regarding VPNs and the simplified internet view, but these are in line with the overall results.

Discussion

This research survey was given to try and gain a base understanding of the general knowledge level on cybersecurity and privacy protection for students at Southeastern Louisiana University. By asking either simplified versions of processes, such as the question on how the internet operated, or by showing things as they would be seen to the participants, such as the question on HTTP versus HTTPS, the goal was to make sure that everyone answering would be able to understand and give their thoughts without being bombarded with technical jargon that they would be unaware of or cause confusion. While some questions, by necessity, did touch on technical concepts, overall, the goal of the survey was met.

From this survey, trends can be seen across the campus in what is an area that can be considered closer to common knowledge and what cannot. Based on the fact that no question was free from individuals who were unsure of the answer or provided wrong responses, even in low quantities such as when asked about a password, all individuals need to be exposed to these concepts in some fashion. These questions were based on scenarios that are encountered by the survey population every day. No individual who answered this survey would not have to use a password to sign in to their student account, email, or learning environment. Most, if not all, will access a computer or similar device and the internet multiple times each day. This gives us our answer to research question number one by showing which concepts in cybersecurity and privacy practices and associated technologies that college students at the Southeastern Louisiana University were familiar with. This also disproves null hypothesis number one by showing that students are not very familiar with many of the concepts presented in the survey overall.

Additionally, while age and time spent in college do not differ in how individuals responded, their major did significantly. Those who were a part of a major that was more likely exposed to, or put them in a position to, have access to information about these concepts, such as computer science, had a higher chance of better understanding the subject area. While this by no means ensured a complete success rate, it did have a significant difference in their responses to many of the ideas compared to other majors and the overall results.

This appears to indicate that those who are not in a technical, technology-focused major are indeed at a disadvantage when it comes to the knowledge of general cybersecurity and privacy practices and how many of the concepts or technologies presented function. While this does not mean that those individuals in a technologically focused major will be completely aware of everything just by being within such a major, it does make sense that they would be more likely to be exposed to these concepts and technologies or explore them on their own. However, this does answer research question number two, in that yes, it does appear that those in a technical major do have a higher base knowledge level. Additionally, this also disproves null hypothesis number two by showing that a student in a technical major does seem to affect the knowledge in the areas of cybersecurity and privacy practices.

The conclusion can be drawn that some type of learning module or course that focuses on explaining the concepts presented in this survey would be advantageous for all students, especially those in non-technical fields. This would allow all students to be better prepared to combat the challenges faced by our increasingly technologically connected world and keep their private information safe at home, school, and in the workplace.

Chapter Summary

Everyone interacts with technology to some degree each day for school, work, and pleasure. However, a core issue is that while technology and the threats posed to those using it continues to grow, many individuals are not exposed to the information they need to protect themselves adequately, their family, and their workplace from those threats. In many cases, ideas and concepts can be misrepresented or misunderstood to the point that an individual may not be aware that they are exposing sensitive information about themselves or information that they would not wish to share to protect their privacy.

This survey highlights several key areas in which the participants were either exposed enough about a subject to make a correct assessment, as seen with a majority answering correctly about the most secure password given. Additionally, it shows where technologies were either misunderstood or their benefits conflated, as seen with VPNs, or that many were simply unsure how to respond at all for a majority of the questions. A discussion of the results from the survey and the combined demographics was given to help show the implications of what the survey and its findings had shown.

In the next chapter, the conclusion to the research dissertation is presented. Recommendations based on the survey results are provided. The limitations of the survey are provided and addressed. Additionally, recommendations for future research directions are suggested.

CHAPTER 5

CONCLUSIONS

The purpose of this study was to explore the general knowledge base of students attending Southeastern Louisiana University. The research intended to quantitatively understand how well these college students understood several key ideas and technologies in the cybersecurity and privacy realm currently in heavy use. By surveying a portion of the student body, a generalized idea of the student body's knowledge level can be estimated.

This chapter presents conclusions based on the survey results and the findings presented in chapter four from both the individual question results and the combination of the demographics with those results. Recommendations for potential solutions for student education are given. Limitations of the research and survey instrument are explored. Finally, future research areas are presented.

Conclusions

From the collected survey results, it does appear that there is a general deficiency in the amount of technical knowledge in the areas of cybersecurity and privacy protection and related technologies for individuals who are outside of a program that is related to these areas. Not everyone needs to be in a program that covers every detail of these ideas, but everyone needs cursory knowledge to continue developing technology.

While some ideas are fairly pervasive and seem to be decently understood, to the best the survey can acknowledge, other areas are very misunderstood, leading to individuals putting themselves into situations where they are exposing themselves to dangerous or invasive circumstances. It is good that most participants were able to identify the strongest password from a list or know that a photo could have location data embedded in it. However, even then, some individuals were unsure or selected incorrect responses. Then when it came to anything that might have a little more technical background to it or not be as straightforward, such as looking at HTTP versus HTTPS or just a general, simplified idea of how the internet works, the number that understood it dropped considerably. While the technical properties of HTTPS do not need to be understood by a majority of the population, the implication of seeing that you are on an encrypted connection should be. The exact way the internet works does not need to be explained in detail to every person. Still, the general idea that you are connecting through a series of servers that various corporations and individuals own should be.

These points need to be understood so that when these students go out into their field of work, they can make informed decisions about when and how to access information. If misunderstood, could a doctor or nurse accidentally violate the Health Insurance Portability and Accountability Act, which most will know simply as HIPAA? Yes, they could mistakenly think they are safe when connecting to information about a patient on an insecure network. An executive could give away insider company information in the same manner, or a Politician could give away national secrets or make laws under false assumptions on a technology they misunderstood. While seemingly extreme, these are not farfetched scenarios if proper education on these topics is not integrated into different programs at some level.

Recommendations

Since this research was focused on college students, there are several solutions to help with this problem. The most straightforward solution is simply integrating a course into the general required curriculum that covers the basic ideas behind these technologies that all students must take. Dupuis proposed a similar solution in their paper, and while some recommendations for this type of course align with their recommendations, several learning methods do not.

This course does not need to be a technically in-depth course and instead can be focused on the surface-level information that most individuals will need to know. This process of staying on the near-surface level of important cybersecurity or privacy protection areas serves multiple duties. The main reason to do so is not to overwhelm or bore any student with exceedingly technical information that may be irrelevant to their chosen major or touch on completely foreign subjects and keep subjects as relevant as possible to them. This would keep the students engaged with the course and learning rather than tuning out because something is irrelevant. While it isn't completely possible to remove all technical aspects, simply due to the nature of the subject matter, removing much of the barrier to entry to gaining more information on the subjects should focus. This approach's secondary goal is that a large berth of material can be covered and maintained to the level of the participants. Additionally, it can revolve around information relevant to them at the time, though course materials required for this approach will be touched on more shortly.

A dynamic approach to the course material must be taken so that it does not become mired in an outdated textbook but instead can adapt and change as quickly as the technology that is being approached in the course does. Finding and using a traditional textbook is likely not the correct solution and may be difficult to find an appropriate one (Dupuis, 2017). While a custom one could be created, as suggested by Dupuis, replacement timelines and policies would need to be considered to ensure it doesn't become irrelevant. A proposed solution would be to use online resources that are already freely available or provided by the host university. Since the proposed solution does not require any deep technical knowledge, resources for the course do not necessarily need to be from a technical journal. Still, instead, a normal news article detailing a breach could be used. This allows for relevant information to be the mainstay for the course, keeps the information up-to-date and relevant to current events, and has the benefit of lowering the cost associated with the course to interested students.

Ideally, this type, of course, could be taken early in a student's college residency. However, the information could also potentially be integrated throughout a program's coursework. Instead of a single course being dedicated to it, the program itself works as a whole to make sure that all of the knowledge needed is gained. This has the potential to be useful for majors that have special considerations that must also be covered, which again can be seen with healthcare and HIPAA. However, care must be taken that topics are not lost in the more specialized focus that some of this instruction would require and that adequate coverage is still provided.

A combination of the general course for every student and then individual majors focusing on their specific needs could potentially yield the best outcome for everyone. This would ensure an even, base-level knowledge across the board of all students, plus the extra information needed in specific majors. This could also be accomplished by sections of the general course being created specifically for different majors to add topics related to that major if there is a high need for it. Not all majors need a special section, but there are cases where it could be appropriate.

Limitations

The biggest limitation of this survey was the population's location. The results found apply specifically to the knowledge base of Southeastern Louisiana University students. Since there are no students from other schools or universities, conclusions that include college students from other locations cannot be drawn. There may be similarities in other schools. However, looking at those is outside of the scope of this paper.

Additionally, since this survey looked only at current college students, the conclusions and recommendations do not apply to individuals who have not yet reached the college level, have already left the education system, or never entered it at all. A different solution would need to be explored for students who are still in the K-12 education system, and another different solution for those already in the workplace.

Finally, changes to the survey instrument used could potentially yield better results. While it is important to know how much an individual knows about all the ideas and technologies mentioned, some could have been better presented. For instance, instead of citing specifically and only HTTPS, the survey could have referenced the lock icon that most modern browsers show when a connection is secure. This would likely be slightly more familiar to some as it would be what they are used to seeing in their browser rather than the full address of many sites. Additionally, finding out which individuals used the private browsing mode of a browser or a VPN in addition to asking them what they did would help find out who does not use them at all and help filter their results with those who do use them. This could potentially give a better understanding of who uses these technologies and understands them, who uses them but has misunderstood or doesn't understand them, and who doesn't use them at all. Questions related to knowing the "why" behind some responses would likely help as well, such as asking a question that prompted the participant to explain why a given password was more secure. The "why" questions could help differentiate between guesses, habits, and actual understanding.

For the demographic portion of the survey, giving a specific choice of major, department, or college rather than having the participant enter their major on their own would likely yield more consistent results. If taken to the department level instead of individual major, it could be more applicable across different Universities that may not offer the same majors.

Future Research

There is a lot that can still be and needs to be explored in this research area. The population is one area that there are several directions to expand. Additional schools can be surveyed, and more regions, different types of schools, etc., could all be looked surveyed. This could allow for different areas of the country to be compared against each other, for two-year and four-year colleges to be compared, for colleges and technical schools to be compared, and much more.

Instead of solely looking at college students, this research could also be expanded into businesses or K-12 grade students. This would allow for further exploration in age ranges, different usage habits, and thoughts on sharing information.

An implementation of a course, as mentioned in the previous section, could be implemented and observed. Students could participate in the course and see how it affects their habits and knowledge in these areas.

REFERENCES

Abd Rahim, N., Hamid, S., Kiah, L., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. Kybernetes, Volume 44 Issue 4, pp. 606-622.

Accreditation Board for Engineering and Technology. (n.d.). Retrieved from https://www.abet.org/accreditation/.

Achee, B. (2021). Leveraging a virtual pre-college summer coding day camp to promote DEI (Diversity, Equity and Inclusion) in recruiting students to Computer Science and Information Technology. Manuscript submitted for publication.

Ahmad, T. (2020). Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. Available at SSRN: https://ssrn.com/abstract=3568830.

Barlett J., Kotrlik, J., & Higgins, C. (2001). Organizational research: Determining appropriate sample size in survey research. Information Technology, Learning, and Performance Journal, 19(1), 43.

Cochran, W. G. (1977). Sampling techniques (3rd ed.). New York: John Wiley & Sons.

Cox, J. (2019). Revealed: Microsoft Contractors Are Listening to Some Skype Calls. Retrieved from https://www.vice.com/en_us/article/xweqbq/microsoft-contractors-listen-to-skype-calls.

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches: Sage publications.

Cyber Innovation Center (n.d.). Cyber.org: The Academic Initiative of the Cyber Innovation Center. Retrieved from https://cyber.org/.

CybHER. (n.d.). Retrieved from https://www.cybher.org/.

D'Anastasio, C., & Mehrotra, D. (2019). The Creators Of Pokémon Go Mapped The World. Now They're Mapping You. Retrieved from https://kotaku.com/the-creators-of-pokemon-go-mapped-the-world-now-theyre-1838974714.

Dark, M., Daugherty, J., Dark, R., Albright, H., Brown, D., Emry, M., & McCallen, A. (2021). GenCyber 5-Year Evaluation. Retrieved from https://www.gen-cyber.com/.

Davis, A. (2015). Cyber security skills for a digital future. New Statesman, 144(5280), 44-45.

Divito, M. (2017). Lesson Learned In Teaching Pre-college Students Cybersecurity. 2017 International Conference on Computational Science and Computational Intelligence (CSCI). Las Vegas, NV, USA, 2017. pp. 1187-1190. DOI: 10.1109/CSCI.2017.208.

Dupuis, Marc J. (2017) "Cyber Security for Everyone: An Introductory Course for Non-Technical Majors," Journal of Cybersecurity Education, Research and Practice: Volume 2017, Number 1, Article 3. Retrieved from https://digitalcommons.kennesaw.edu/jcerp/vol2017/iss1/3.

Dreibelbis, R. C. (2016). It's More Than Just Changing Your Password: Exploring the Nature and Antecedents of Cyber-Security Behaviors. Retrieved from https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=7279&context=etd.

European Union Agency for Cybersecurity. (2020). ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected. Retrieved from https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020/.

Furman, S. M., Theofanos, M. F., Yee-Yin Choong, B., & Stanton, B. (2012). Basing Cybersecurity Training on User Perceptions. Security & Privacy, IEEE, Volume 10 Issue 2, 40-49.

GenCyber. (n.d.). Retrieved from https://www.gen-cyber.com/.

Haislip, J., Kolven, K., Pinsker, R., Steffen, T. (2019). The Economic Cost of Cybersecurity Breaches: A Broad-Based Analysis. The 2019 Workshop on the Economics of Information Security. Retrieved from https://weis2017.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_13.pdf.

Hoggard, A. (2014). Comparing Canadian and American Cybersecurity Awareness Levels: Educational Strategies to Increase Public Awareness. ProQuest Dissertations Publishing.

IBM Security & Ponemon Institute. (2020). Cost of a Data Breach Report 2020. Retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.

Israel, G. (1992). Determining Sample Size. University of Florida, PEOD-6. Retrieved from https://www.academia.edu/21353552/Determining_Sample_Size_1.

Jayakumar, P., Brohi, S. N., & Zaman, N. (2020). Top 7 Lessons Learned from COVID-19 Pandemic (Version 1). TechRxiv. https://doi.org/10.36227/techrxiv.12264722.v1.

Katsantonis, M., Fouliras, P., & Mavridis, I. (2017). Conceptual analysis of cyber security education based on live competitions. IEEE Global Engineering Education Conference. pp. 771-779.

Mache, J., & Weiss, R. (2018). Hands-on cybersecurity exercises. Journal of Computing Sciences in Colleges, Volume 34, Issue 1, pp. 231-232.

Mandal, S., & Khan, D. A. (2020). A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic. 2020 International Conference on Smart Electronics and Communication. DOI: 10.1109/ICOSEC49089.2020.9215374.

McNulty, M., & Kettani, H. (2020). On Cybersecurity Education for Non-technical Learners. 3rd International Conference on Information and Computer Technologies, San Jose, CA, USA, pp. 413-416.

National Security Agency. (n.d.). National Centers of Academic Excellence in Cybersecurity. Retrieved from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/.

Neigel, A., Claypoole, V., Waldfogle, G., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. Volume 92. Computers & Security. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404820300183.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

Office of the Australian Information Commissioner. (2019). Notifiable data breaches scheme 12-month insights report. Sydney: OAIC. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/.

Olmstead, K., & Smith, A. (2017). What the Public Knows About Cybersecurity. Retrieved from https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/.

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a Cybersecurity Workforce and Aware Public. Security & Privacy, IEEE, 10(3), 76-79.

Poyraz, O.I., Canan, M., McShane, M., Pinto, C., & Cotter, T. (2020). Cyber assets at risk: monetary impact of U.S. personally identifiable information mega data breaches. The Geneva Papers on Risk and Insurance - Issues and Practice. Volume 45. pp. 616-638. https://doi.org/10.1057/s41288-020-00185-4.

Pye, K. (2016). Teaching Cybersecurity in K-12 Schools. ProQuest Dissertations Publishing.

Raigoza, J. (2018). An Experience Report on Running a Pre-College Computer Science Summer Program. 2018 International Conference on Computational Science and Computational

Intelligence (CSCI). Las Vegas, NV, USA, 2018. pp. 655-658. DOI: 10.1109/CSCI46756.2018.00131.

Ricci, J., Breitinger, F., & Baggili, I. (2018). Survey results on adults and cybersecurity education. Education and Information Technologies: Springer Science & Business Media. pp. 1-19.

Robot, Marvin the. (2016). Elderly people online: habits and concerns. Retrieved from https://me-en.kaspersky.com/blog/older-people-internet/5593/.

Rowland, P., Podhradsky, A., & Plucker, S. (2018). CybHER: A Method for Empowering, Motivating, Educating and Anchoring Girls to a Cybersecurity Career Path. Proceeding of the 51st Hawaii International Conference on System Sciences. pp. 3727-3735. Retrieved from http://hdl.handle.net/10125/50358.

Scheponik, T., Sherman, A. T., Delatte, D., Phatak, D., Oliva, L., Thompson, J., & Herman, G. L. (2016). How students reason about Cybersecurity concepts. Vol. 2016, pp. 1-5.

Schwartz, S. (2018). Schools Teach 'Cyber Hygiene' to Combat Phishing, Identity Theft. In Vol. 84, pp. 4-9: Prakken Publications.

Skinner, G. (2017). Cyber Security Education for Children Using CALC (Cloud Adaptive Learning Courses): A Position Paper on Cyber Security for Younger Demographics. Annual International Conference on Infocomm Technologies in Competitive Strategies, 50-56.

Smith, C. (2018). Cyber Security, Safety, & Ethics Education. ProQuest Dissertations Publishing.

Southeastern Louisiana University Office of Institutional Research. (2019). Undergraduate & Graduate Students by Age and Gender. Retrieved from https://www2.southeastern.edu/Administration/Inst-Research/Student/data.cgi?stuage.txt.

Southeastern Louisiana University Office of Institutional Research. (2020). Enrollment by Major. Retrieved from https://www2.southeastern.edu/Administration/Inst-Research/Acadprog/data.cgi?majors.txt.

Southeastern Louisiana University Office of Institutional Research. (2020). General Information. Retrieved from https://www.southeastern.edu/about/general/.

Southeastern Louisiana University Office of Institutional Research. (2020). Semester Registration Report Fall 2020. Retrieved from https://www.southeastern.edu/admin/ir/srr/files/fall_2020.pdf.

Southeastern Louisiana University Office of Technology. (2019). Report on Phishing, Malware, Suspended Accounts, and Rogue Access Points. Unpublished manuscript.

Symantec. (2017). Internet Security Threat Report. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.

Symantec. (2019a). Internet Security Threat Report. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.

Symantec. (2019b). Monthly Threat Report. September 2019. Retrieved from https://www.symantec.com/security-center/publications/monthlythreatreport.

Thompson, J. D., Herman, G. L., Scheponik, T., Oliva, L., Sherman, A., Golaszewski, E., Phatak, D., & Patsourakos, K. (2018). Student Misconceptions about Cybersecurity Concepts: Analysis of Think-Aloud Interviews. In 2018 Volume of the Journal of Cybersecurity Education, Research and Practice.

U.S. Bureau of Labor Statistics. (2020). TED: The Economics Daily. May 22, 2020. Retrieved from https://www.bls.gov/opub/ted/2020/66-point-2-percent-of-2019-high-school-graduates-enrolled-in-college-in-october-2019.htm.

Valentino-DeVries, J., Singer, N., Keller, M., & Krolik, A. (2018). Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret. New York Times.

Verizon. (2020). Analyzing the COVID-19 data breach landscape. Retrieved from https://enterprise.verizon.com/resources/articles/analyzing-covid-19-data-breach-landscape/.

Verizon. (2020). Verizon Data Breach Investigation Report. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/.

Wang, P., D'Cruze, H., David, W. (2019). Economic Costs and Impacts of Business Data Breaches. Issues in Information Systems. Volume 20. Issue 2. pp. 162-171. https://doi.org/10.48009/2_iis_2019_162-171.

The White House. (2016). Executive Order – Commission on Enhancing National Cybersecurity. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity.

APPENDIX A: SURVEY

The following is the survey presented to participants in this research.

1. What is your age?

    - Under 18
    - 18-21
    - 22-25
    - 25-30
    - 30-35
    - 35+

2. What is your gender?

    - Female
    - Male
    - Prefer not to say.
    - Other:

3. What is your current classification?

    - Freshman
    - Sophomore
    - Junior
    - Senior
    - Graduate Student
    - Other:

4. What is your current major? (Ex. Nursing)

5. How does information travel from your computer to a website?

- Directly from my computer to the website.
- From my computer, to my router, to the website.
- From my computer, through a series of other computers, to the website.
- Not sure of answer.

6. Which of the following is true about a "Private Browsing" feature in an internet browser? (Choose all that apply)

- Information such as browsing history will not be stored by the browser.
- Internet Service Providers cannot see your online activity.
- It automatically encrypts your connection.
- Not sure of the answer.

7. What is the difference between a website having "https://" at the beginning of it versus "http://" (without the 's')? (Choose all that apply)

- Traffic to and from the website is encrypted.
- The website is up-to-date.
- The website contains no viruses.
- The website has a special version available.
- None of the others.
- Not sure of the answer.

8. Which of the following passwords is the most secure?

- Ht$j7PKw

- Marker1$
- selu1234
- 12345678
- Not sure of answer.

9. Turning off the GPS function of your smart device (such as phone, tablet, laptop) will keep your location from being tracked.

- True
- False
- Not sure of the answer.

10. The location that a photo was taken could be embedded in the photo itself.

- True
- False
- Not sure of the answer.

11. When using an application on any device, the permissions you allow it to have should...

- always be carefully considered and blocked if they don't make sense for the specific application.
- be accepted because the application knows what it needs.
- be an all or nothing choice.
- Not sure of answer.

12. All Wi-Fi traffic is encrypted by default on all wireless routers.

- True
- False
- Not sure of the answer.

13. Public Wi-Fi networks (such as at an airport, restaurant, or school) that requires a password to access is generally safe to use for personal activities such as online banking or other sensitive exchanges.

- True
- False
- Not sure of the answer.

14. A Virtual Private Network (VPN) can help minimize what type of cybersecurity risk? (Choose all that apply)

- Use of insecure networks.
- Phishing attacks
- Tracking by website operators
- De-anonymization by network operators
- Keylogging
- Not sure of the answer.

APPENDIX B: UNIVERSITY STUDENTS BY AGE AND GENDER

	2015	2016	2017	2018	2019
Female					
Under 18	1,622	1,716	1,521	1,520	1,405
18-19	2,480	2,595	2,736	2,808	2,798
20-21	2,042	2,026	1,912	2,032	2,194
22-24	1,420	1,373	1,383	1,319	1,293
25-29	665	628	627	605	603
30-34	317	281	282	263	259
35-39	198	190	206	160	160
40-49	235	190	209	218	203
50-64	117	102	101	90	87
65 and Over	16	13	16	21	24
Total	9,112	9,114	8,993	9,036	9,026
Male					
Under 18	978	964	939	914	849
18-19	1,505	1,528	1,586	1,629	1,597
20-21	1,240	1,218	1,179	1,228	1,262
22-24	989	962	931	905	933
25-29	451	415	396	342	333
30-34	146	129	119	104	100
35-39	66	70	61	65	48
40-49	70	58	71	68	66
50-64	27	28	23	23	33
65 and Over	10	13	10	13	13

Total	5,482	5,385	5,315	5,291	5,234
Total					
Under 18	2,600	2,680	2,460	2,434	2,254
18-19	3,985	4,123	4,322	4,437	4,395
20-21	3,282	3,244	3,091	3,260	3,456
22-24	2,409	2,335	2,314	2,224	2,226
25-29	1,116	1,043	1,023	947	936
30-34	463	410	401	367	359
35-39	264	260	267	225	208
40-49	305	248	280	286	269
50-64	144	130	124	113	120
65 and Over	26	26	26	34	37
Total	14,594	14,499	14,308	14,327	14,260

APPENDIX C: ENROLLMENT BY MAJOR

Departments and Majors	Fall 2020
College of Arts, Humanities & Social Sciences	
Communication & Media Studies	
BA Communication	260
MA Organizational Communication	31
Department Total	291
English	
BA English	104
BA English Education	64
MA English	22
Department Total	190
General Studies	
BGS General Studies	533
Department Total	533
History & Political Science	
BA History	129
BA Political Science	88
BA Social Studies Education	82
MA History	27
Department Total	326
Music & Performing Arts	
BM Music	114
MMU Music	15
Department Total	129

Psychology	
BA Psychology	583
MA Psychology	34
Department Total	617
Sociology & Criminal Justice	
BA Criminal Justice	439
BA Sociology	58
MS Applied Sociology	23
Department Total	520
Visual Art + Design	
BA Art	358
World Languages & Cultures	
BA Spanish	1
BA World Languages	26
Department Total	27
College Total	2,845
College of Business	
Accounting & Finance	
BS Accounting	414
BS Finance	154
Department Total	568
Management & Business Administration	
BBA Business Administration	605
BA Management	440
PBC Business Administration	0
Department Total	1,045

Marketing & Supply Chain Management	
BA Marketing	373
BS Supply Chain Management	71
Department Total	444
MBA	
Total	100
College Total	2,157
Center for Student Excellence	
Undecided	2,523
College Total	2,523
College of Education	
Educational Leadership & Technology	
M.Ed. Educational Leadership	81
Ed.D. Educational Leadership	98
Department Total	179
Teaching & Learning	
BS Early Childhood Education	277
BS Elementary Education	221
BS Elementary Education & Special Education	59
BS Middle School Education	89
BS Middle School Education & Special Education	11
M. Ed. Curriculum & Instruction	20
M. Ed. Special Education	25
MAT Elementary Education	8
MAT Special Education: Early Interventionist (Birth-5)	10

Department Total	720
Other	
Add-on Certification	45
Alternate Certification	17
Lions Connected	19
Masters Plus 30	2
Other Total	83
College Total	1,186
College of Nursing & Health Sciences	
Health & Human Sciences	
BS Communication Science Disorders	173
BS Family and Consumer Sciences	223
BS Health Management Systems	159
BA Social Work	257
MS Child Life	14
MS Counseling	97
M. Ed. Counselor Education	N/A
MS Communication Science Disorders	55
Department Total	978
Kinesiology & Health Studies	
BS Athletic Training	91
BS Heath Education & Promotion	16
BS Health & Physical Education	58
BS Health Sciences	126
BS Kinesiology	626
BS Sports Management	142

MA Health and Kinesiology	N/A
MS Health & Kinesiology	34
Department Total	1,093
School of Nursing	
BS Nursing	N/A
BSN Nursing	1,470
Master's Nursing (MSN)	104
Doctorate Nursing Practice (DNP)	34
PMC Family Nurse Practitioner	0
PMC Psychiatric Mental Health Nurse Practitioner	17
Department Total	1,625
College Total	3,638
College of Science & Technology	
Biological Sciences	
BS Biology	776
MS Biology	22
Department Total	798
Chemistry & Physics	
BS Chemistry	106
BS Physics	39
Department Total	145
Computer Science	
BS Computer Science	271
BS Information Technology	124
Department Total	395
Industrial & Engineering Technology	

AAS Industrial Technology	49
BS Engineering Technology	292
BS Industrial Technology	170
BS Occupational Health, Safety & Environment	131
Department Total	642
Mathematics	
BS Mathematics	74
Department Total	74
MS Integrated Sciences & Technology	19
College Total	2,073
Other	
Special Program for Adults	22
Extended Studies	17
University Total	14,461

APPENDIX D: ALL PARTICIPANT MAJORS

Reported Major	Count
Accounting	34
Accounting and Finance	2
Art	3
Athletic Training	1
Biochemistry	3
Biological Sciences	5
Biology	32
Biology and Pre-Med	1
Business	12
Business Administration	27
Business Management	7
Business Marketing	2
Cellular and Molecular Biology	1
Chemistry	7
Child Life	4
Clinical Mental Health Counseling	2
Communication	14
Communication Sciences and Disorders	18
Computer Science	25
Counseling	6
Criminal Justice	28
Curriculum and Instruction	1
Doctoral Candidate	1
Dual Major: Accounting and Finance	1

Dual Major: History and Political Science	1
Dual Major: Plant Science and Photography	1
Dual Major: Sociology and Criminal Justice	1
Early Childhood Education	16
Ecology	1
Education	15
Educational Diagnostician Certification	1
Educational Leadership	11
Electrical Energy Engineering Technology	1
Elementary Education	8
Engineering Technology	2
English	12
English Education	3
Entrepreneurship	1
Exercise Science	1
Family and Consumer Science	10
Finance	8
Fine Art	1
General Studies	23
Gifted Education	1
Graphic Design	10
Health and Nutrition	1
Health and Physical Education	1
Health Science	8
Health Studies	2
Health Systems Management	9
History	17

Human Resource Management	4
Industrial Technology	8
Industrial/Organizational Psychology	1
Information Technology	11
Integrative Biology	10
ISAT	1
Jazz Studies	1
Kinesiology	44
Management	6
Marketing	18
Mass Communications	2
Math Education	2
Mathematics	6
MBA	10
Mechanical Engineering	1
Mechatronics Engineering	1
Microbiology	4
Middle School Education	1
Middle School English Education	1
Music	2
Music Education	3
Music Performance	3
No Response	1
Nursing	107
Nursing Education	1
Nutrition	1
Occupational, Safety, Health, and Environment	13

Organizational Communication	4
Painting	1
Pharmacy	1
Physical Education	1
Political Science	10
Political Science Pre-Law	1
Pre-Med	1
Psychology	55
Publications	1
School Counseling	1
Science	1
Secondary English Education	1
Secondary Social Studies Education	1
Small Business Management	1
Social Studies Education	7
Social Work	19
Sociology	8
Special Education	6
Speech Language Pathology	1
Sport Management	10
Supply Chain Management	3
Teaching	2
Teaching and Learning	1
Theater Design	2
Undecided	1
Veterinary Medicine	1
Visual Art	1

Vocal Music Education	1
Vocal Performance	1

APPENDIX E: CLASSIFICATIONS FOR TOP TEN MAJORS

Classification	Reported Major	Count
Freshman	Accounting	3
Freshman	Biology	7
Freshman	Business Administration	4
Freshman	Computer Science	4
Freshman	Criminal Justice	7
Freshman	General Studies	2
Freshman	Kinesiology	7
Freshman	Nursing	36
Freshman	Psychology	12
Freshman	Social Work	3
Sophomore	Accounting	6
Sophomore	Biology	6
Sophomore	Business Administration	6
Sophomore	Computer Science	8
Sophomore	Criminal Justice	7
Sophomore	General Studies	1
Sophomore	Kinesiology	9
Sophomore	Nursing	23
Sophomore	Psychology	14
Sophomore	Social Work	5
Junior	Accounting	8
Junior	Biology	11

Junior	Business Administration	4
Junior	Computer Science	2
Junior	Criminal Justice	3
Junior	General Studies	6
Junior	Kinesiology	10
Junior	Nursing	18
Junior	Psychology	12
Junior	Social Work	6
Senior	Accounting	17
Senior	Biology	4
Senior	Business Administration	8
Senior	Computer Science	10
Senior	Criminal Justice	11
Senior	General Studies	13
Senior	Kinesiology	15
Senior	Nursing	19
Senior	Psychology	10
Senior	Social Work	5
Graduate Student	Biology	4
Graduate Student	Business Administration	5
Graduate Student	Computer Science	1
Graduate Student	Kinesiology	2
Graduate Student	Nursing	9
Graduate Student	Psychology	7
Other	General Studies	1

Other	Kinesiology	1
Other	Nursing	2