NAME: **Ricardo Gonzalez**

PARENTS' NAMES **Ricardo and Maria Gonzalez**

HOMETOWN: **Greenwood, Indiana**

CAREER OBJECTIVE**: I want to work for a consulting firm within the world of Cybersecurity.**

BIOGRAPHY: **I am a first-generation university student with a vast interest in computers and computer systems. The security of these systems has been of great interest to me, since I begin my journey at Purdue. I want to assure that all students, friends, and family know the dangers of improper computer security. I hope to one day be able to work as a computer security consultant in order to allow companies to not have to worry about their cybersecurity needs.**

FACULTY LSAMP SPONSOR: **Dr. Dennis Buckmaster, Professor of Agricultural and Biological Engineering**

GOAL OF THE WORK: **This research was done in order to see how many students were unaware of the potential for certain Cybersecurity crimes.**

PERSONAL STATEMENT ABOUT THE LESSONS LEARNED FROM THIS EXPERIENCE: **The lessons I learned from this experience were like no other. Without minimal help from a faculty member, I was in charge of assuring all aspects of the research assignment were met. I learned how to properly manage my time, in order to meet all deadlines in a prompt manner. I was also in charge of all of the data which allowed me to understand how to present the data in a proper fashion.**

Purdue University Students' Perceptions of Cybersecurity

By Ricardo Gonzalez

Abstract

An investigation into Purdue University students' attitudes about cybersecurity was conducted. Students were asked about their thoughts on cybersecurity, cyber-terrorism, and how they protect themselves. The data indicated that students were both aware of cyber-threats and participated in potentially unsafe internet activities. A variety of misconceptions regarding online security exposed, highlighting the need for greater education for college students regarding staying safe during online activities.

Keywords

college students; cybersecurity; cyber terrorism; online protection; perception of safety; unsafe web activities

Introduction

This paper presents the author's experiences during a faculty-directed research program through the Louis Stokes Alliance for Minority Participation (LSAMP) project under the supervision of Dr. Dennis Buckmaster of Agricultural & Biological Engineering to understand college students' perceptions of cybersecurity. In a world dominated by technology, cyber-attacks have become an ever-increasing threat to society. The growing dependence on technology within an individual's day-to-day life has resulted in the sudden increase of cyber-attacks and online crimes happening daily. As a result, many people are unaware of the variety of cyber-attacks, or even how to protect themselves from becoming a victim to an attack. Most college students are unable to distinguish the difference between cyber-attacks and cyber terrorism, resulting in many students becoming far too comfortable online.

In a research study done by Powlowski and Jung (2015), it was found that cyber-attacks and cyber terrorism have become vastly more prevalent as

technology advances. Powlowski and Jung further demonstrated that over 100,000 individual attacks occurred in 2015 alone, and cyber-attacks continue to increase each year. These attacks often go undetected, because cyber-attack numbers are intricate and essentially untraceable. As a result, people are not aware of these attacks until it's too late. For example, Larson and Pagliery (2017) discuss an incident of ransomware, a type of cyber-attack, that occurred in February of 2017 at the Hollywood Presbyterian Hospital in Los Angeles, California. The attack resulted in the loss of access to patient and doctor records for two weeks, forcing them to pay the bitcoin equivalent of roughly $17,000 to retrieve their data.

Research done by Luker and Peterson (2003) shows that many students on college campuses do not know what cybersecurity is, what cyber-attacks are, or how dangerous they can be. They further explain how some attacks on schools were perpetuated by students to scare the rest of the campus. Therefore, they concluded that there should be a general collegiate-level education course on cybersecurity at all schools. This course should teach students what they need to look out for online, as well as how to protect themselves. This previous study will be useful in the current research, because it will allow a comparison of the Luker and Peterson (2003) research results with the current survey results from the Purdue University students. Aslani et al. (2017) have shown that most attacks that happen to colleges around the country are done by students from within the school's network. The general student population feels comfortable with the fact that school networks may never be attacked from the outside, but the real danger typically lies within the school.

This research will expand on the previous studies, and more specifically, look into college students' perceptions and possible misconceptions of cybersecurity and cyber-terrorism at Purdue University. A qualitative methodology will be used to understand the perceptions of Purdue University students in regards to cybersecurity. This study will ask the following primary research questions:

1. How many college students have a false sense of cybersecurity? (i.e. students who feel they are safe, but are at significant risks online?)

2. How do college students define cyber-terrorism?

3. Are college students protecting themselves online? If so, what are they doing to stay safe?

In order to collect data in the most effective way amongst a large group of students, an online survey was used. This research was performed as part of an undergraduate class project. No individualized data were kept, and the only results retained are those present in this paper.

Methods

The Survey

A Qualtrics® survey was used to gather qualitative data about Purdue University students' perceptions of cybersecurity. The researchers asked a variety of questions that involved trying to figure-out the general knowledge that students have on this important topic. The researchers then continued to ask more specific questions regarding how often the students spend time online, what websites they most commonly visit and use, and some of their more common internet habits. Throughout the survey, there are different question types, such as multiple choice, free response, and ranking questions. These questions helped get a better idea of the perceptions and possible misconceptions that college students might have regarding cybersecurity and cyber-terrorism.

The survey was made and distributed through Qualtrics®. The researchers chose Qualtrics®, not only because it is reliable, but because it also aids in the storage of data in an online database, making it easy to retrieve at a later time. Qualtrics® is also very easy for researcher users to access and understand, being commonly available on both mobile and PC platforms for the K-12 and higher education communities.

Participants

The researchers surveyed 42 current students of Purdue University, with ages ranging from 18 to 25 years old and backgrounds in a variety of majors. Since this wok was conducted over the summer, it was difficult to find many students on campus, who were willing to take the survey. Because of this, the researchers distributed the survey through social media websites such as Facebook® and GroupMe® to get the most participants possible.

Data Analysis

Do college students have a false sense of cybersecurity? (i.e. students who feel they are safe but are at significant risks online?)

The researchers have discovered through this study, that there are a significant number of college students that have serious misconceptions about cybersecurity. For this particular question, the researchers had expected the students to respond by saying that they did in fact have a false sense of security regarding online activities. The survey included three questions used to determine the misconceptions amongst college students. The first question was, "How comfortable do you feel online?" As shown below in Figure 1, the majority of the participants felt at least somewhat comfortable online. Taking a closer look into this data, fifty percent of the participants said that they felt somewhat comfortable online, while an additional forty-one percent claimed to feel extremely comfortable online.

This information is worth highlighting, because ninety percent of

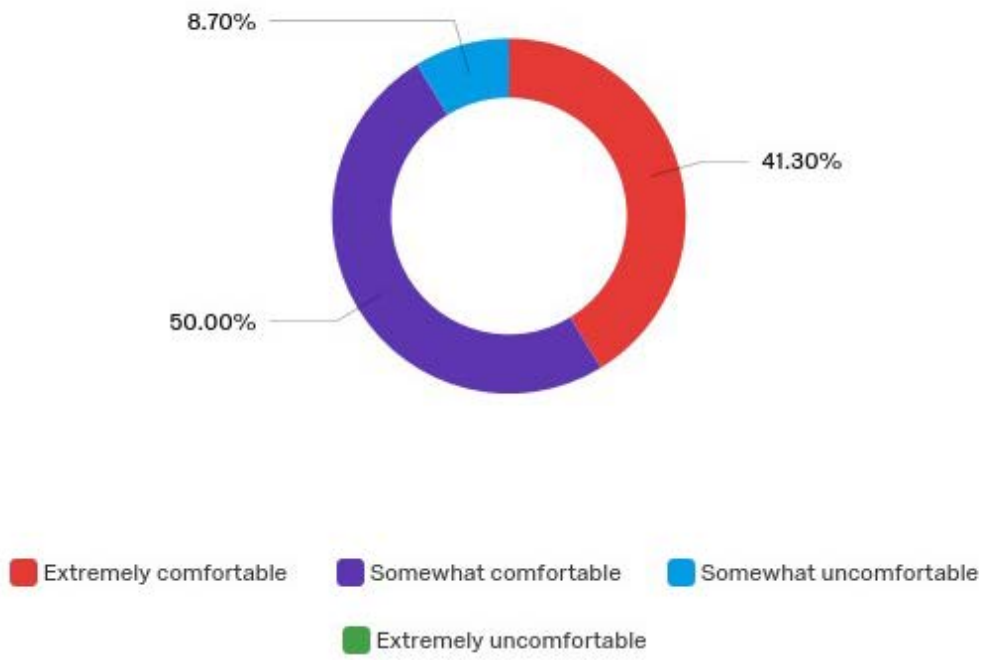

Figure 2 - Purdue student survey results for "How comfortable do you feel online?"

the participants felt comfortable online, regardless of cyber threats. According to Holt and Kilger (2012), the evolution of technology has completely changed how the world communicates, causing cyberspace to become a key target for politically motivated attacks and other social conflicts. This work demonstrated that many students reported a willingness to engage in traditional forms of nonviolent political actions, expressing their opinions on social media platforms such as Facebook®. However, the data from the current survey shows that regardless of the growing sophistication of cybercrimes, college students still feel rather comfortable online, perhaps overly so.

The second survey question asked participants if they had ever saved any of their personal information online, and their responses are seen in Figure 2. Before administering the survey, the researchers had expected a majority of the participants to admit to having saved

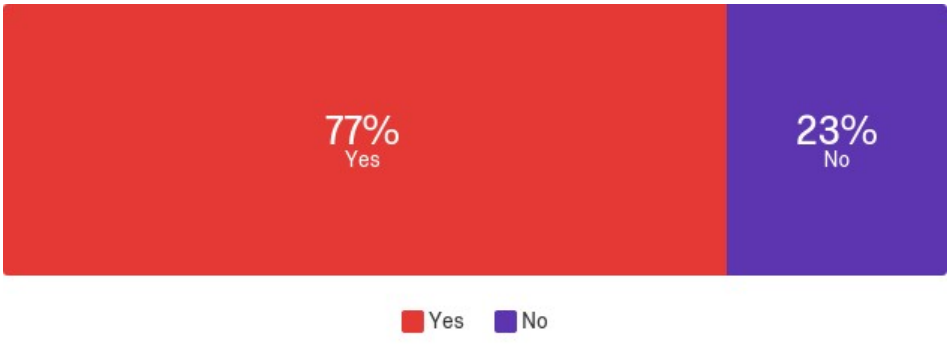

Figure 1 - Purdue student survey results for "Have you ever saved your personal information online?"

their personal information online. Looking at the data in the chart, it is clear that the researcher expectations prior to the survey were correct, because seventy-seven percent of the participants claimed that they had saved their personal information online. It is clear from the current study that college students heavily rely on websites and social media platforms to store their personal information, with no fear that these websites could be hacked or their personal information stolen. However, according to O'Brien (2016), even very popular and protected websites can be attacked without warning through a cyber-attack, such as DDoSing, which causes an increasing and overwhelming flow of traffic through a specific website, causing it to become unusable and vulnerable to outside influence. There is an endless list of different cyber-attacks that could result in rendering a website inaccessible and exposed.

The last question asked addressed any misconceptions amongst college students about performing actions online, and participants were required to check-off all the actions they recall performing. The options included within the survey were saving usernames and passwords, saving credit card information on a phone or computer, opening "clickbait" emails or articles, giving-out their personal information to someone online, downloading any unprotected music or video files, or sharing their location online.

The data from Figure 3 showed that twenty-seven percent of college students have saved usernames and or passwords online, and twenty-five percent of college students reported that they have shared their location online. After comparing this data to the amount of college students who feel comfortable online, the researchers can only conclude that college students are putting themselves at a significant risk of cyber-attacks.

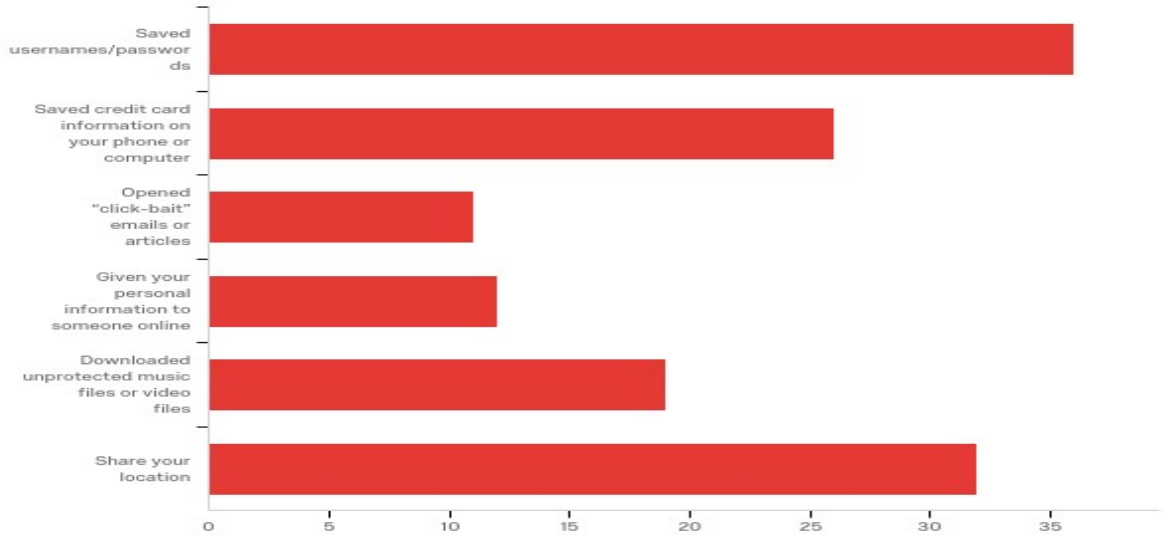

Figure 3 - Purdue student survey results for "Have you done any of the following? (Please check all that apply.)"

College students appear to have a false sense of cybersecurity, believing they are safe online. However, their habits of saving personal information online and sharing their location puts them at high risk of a personal cyber-attack.

How do college students define cyber terrorism?

In this section, the survey participants were asked if they personally felt that they had a stronger knowledge of cybersecurity, cyber-threats, and cyber-terrorism compared to other college student peers. The participants were then asked to define cyber-terrorism in their own words, and their responses were compared in order observe any similarities amongst the answers.

Participants were asked "How much do you feel you know about cyber-threats compared to other college students?", and the results are shown above in Figure 4. Examining the pie chart, over ninety percent of the participants believe that they know more about cyber-threats than their peers. From this result, the researchers concluded that college students are confident regarding their knowledge of cyber-threats and cybersecurity. Prior to the survey, the researchers expected to get a large percentage of the participants believing that they knew more than their peers. Therefore, the researchers decided to follow that question by asking if they had ever heard of the term "cyber-terrorism", and Figure 5 shows these results.

It was a surprise that only eighty-four percent of the researcher participants were familiar with the term, although ninety percent of the survey participants reported they knew more about cyber threats than their peers. Those participants who answered yes, were

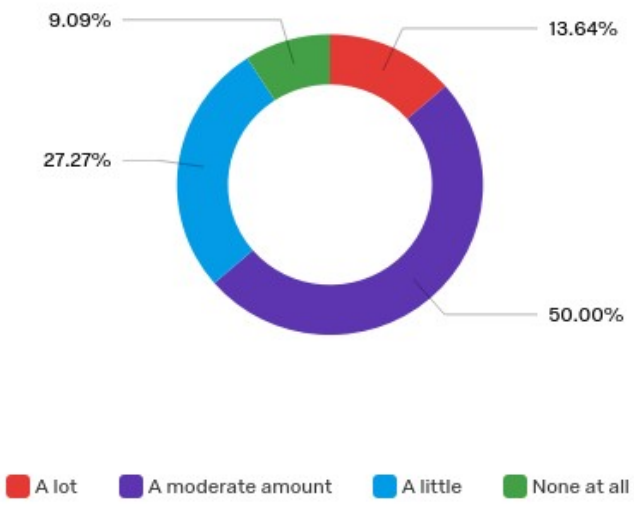

Figure 4 - Purdue student survey results for "How much do you feel you know about cyber threats compared to other college students?"

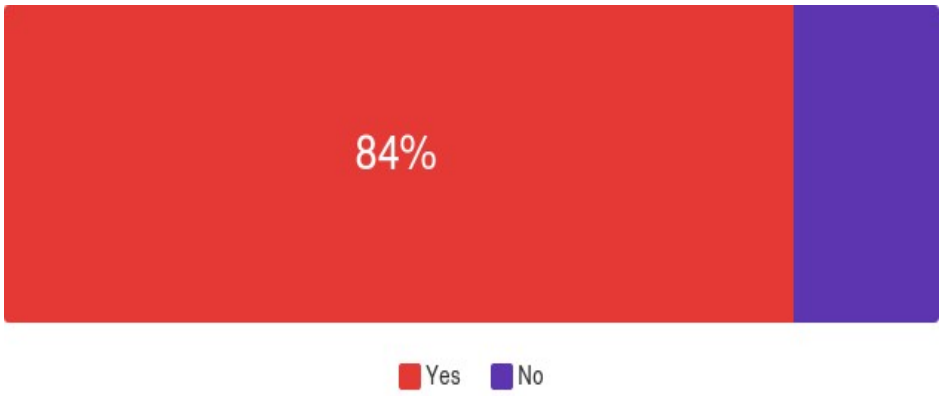

Figure 5 - Purdue student survey results for "Have you heard of cyber-terrorism?"

then asked "What are your initial thoughts when hearing or seeing the term "cyber-terrorism"?" The answers the researchers received differed greatly. Many student responses referred to hacking or cyber theft. For example, some answers were as detailed as "It's a very massive threat to every person, because the internet is so essential to society." or "Large-scale hacking that leads to massive amounts of leaked personal and top secret data."

Aside from the detailed responses, the researchers also received the simplest of answers such as "bad", "hacking", "misunderstood", and "dangerous". The researchers were shocked by the varied responses considering that over ninety percent of the participants had originally claimed they knew more than the average person when it came to cybersecurity. Yet when asked about cyber-terrorism, there was not a clear consensus in their answers. According to Kenney (2015), cyber-terrorism and other cyber-attacks, such as hacktivism or cyber-ware, "...are considered a deliberate, computer-to-computer attack that disrupts, disables, destroys, or takes over a computer system. As well as damaging or stealing the information it contains without the knowledge or consent of the victim." Although the researchers did not expect to receive such a detailed definition of cyber-terrorism, they did expect those who claimed to be knowledgeable regarding cyber-terrorism to provide a better description. This shows a large discrepancy between the college students' perceptions and expert opinion on cybersecurity, cyber-terrorism, and cyber-threats.

Are college students protecting themselves online? If so, what are they doing to stay safe?

In the Purdue student survey, the participants were asked about their online habits and if they protected their data and personal information online. The participants who protected themselves online were then asked what methods they use to keep themselves safe, as well as their information. This data was crucial to the research since it had come to the researcher's attention with the previous survey question that

college students have different perceptions of cybersecurity.

Participants were asked “How are you protecting yourself online? Please provide a brief description of what you do to protect yourself online.” The data collected from this question varied in both length and in what was done to stay safe online. Similar to the previous question, the researchers received a variety of answers such as “Make sure to change my passwords frequently and to try not to share my personal information online to sketchy websites or people I don’t know” and “Never save passwords; operate under pseudonyms; clean computer for viruses regularly.” After analyzing the data, the researchers also discovered that many students have invested in antivirus software. Antivirus software protects them from common malware codes, which are tools used to perform several types of cyber-attacks. Many students even say that they protect themselves by never saving information online such as credit cards and other personal information. Some students have used VPNs, or virtual private networks, which hide I.P. addresses or encrypt them, so hackers cannot steal any information. However, there was a small percentage of college students who did not seem to care much at all about online safety. The researcher team believes that a way to decrease the number of students who are unaware of cyber-attacks and be able to prevent them is by raising awareness on college campuses. Luker and Petersen (2003) suggest that it is necessary to bring an awareness of cyber-attacks and cyber-attack prevention to college students. They argue that by making a mandatory course for all undergraduate students will help keep college students up-to-date on cyber-attacks and specific methodologies of cyber-crime prevention.

Conclusion/Discussion

After analyzing the research data, it was discovered that a false sense of cybersecurity amongst students at Purdue University exists. From these conclusions, the researchers hope to educate more college students about the cyber-threats and cyber-attacks that they put themselves at risk for daily. The researchers believe by increasing the awareness that students have will decrease the number of cyber-attacks now happening to college students.

The researchers can see that 84% of the survey participants have heard of cybersecurity in a vague way. Stating that cyber-terrorism is “bad” does not indicate a true understanding of cyber-terrorism. When asked their initial thoughts of cyber-terrorism, the participants in the survey answered with several different definitions, as well as terms that reminded them of cyber-terrorism. The collected definitions were varied in a such a way that there were no clear similarities amongst the responses. It is clear that college students either have not been educated on cybersecurity and cyber-terrorism, or they do not have the motivation to learn about these topics on their own. However, the results from

research question two showed that the majority of students (roughly 90%) felt confident that they knew more about cyber threats than their peers. Only about 8% of students were honest enough to say that they did not feel they knew more than other students. According to Powlowski (2015) many colleges have not been providing students with cybersecurity courses. These courses have only slowly started becoming available to students in universities nationwide recently. Due to the lack of education on the subject, there may be a large skew within the college students' perceptions of cybersecurity. However, Luker (2003) suggests that the misconceptions college students have on cybersecurity can be changed by educating the students. Creating a mandatory cybersecurity course for students of all majors to take, would not only increase student awareness of the problem on campus, but it could also lead to a decrease in cyber-attacks on college students over the coming years.

Another issue that was highlighted in the survey was the false sense of security that college students have when it comes to the Internet. Nearly all of the participants (over 90%) in the survey said that they felt comfortable online. Yet when later asked about their online habits, such as saving their personal information online or sharing their location, the majority of the research participants had agreed that they had engaged in risky behavior. The main issue with this is that many college students think that all the information they put out there is safe, and they're protected from cyber-threats. With this false sense of security, college students are unknowingly saving their logins, as well as saving personal information like their home addresses and credit card information online to reduce the stress of checking-out when online shopping. By saving information online, this automatically raises the risk of a personal cyber-attack, because it cannot be guaranteed that this information is protected online. This gross misconception puts college students at higher levels of risk of being a victim of ransomware, a computer virus designed to hold data hostage until a specific fee is paid. Once the fee is paid, the virus will give a decryption key, allowing the victim to regain access to their data (Larson & Pagliery, 2017).

The final question the researchers asked was, "What are students doing to protect themselves?" Most things students said they are doing to protect themselves do not completely protect them online. When students say they use antivirus software to protect themselves, it shows that they are not entirely aware of what they are trying to protect themselves from. When it comes to cyber-attacks or cyber-terrorism, a simple antivirus software will not be able to stop hackers from stealing information from computers. An antivirus software only stops certain viruses and occasionally some types of malware. Since college networks are more likely to be attacked from the inside, it is an easy task for someone who is already on the

network to steal information, even with the antivirus software operational on their machines (Aslani et al., 2017). Most of the methods that the students are using to protect themselves are not very effective at keeping their information safe for the long run.

As shown in the data analysis, it is clear that there are several misconceptions and a strong sense of false security regarding safety online and amongst college students at Purdue. Hopefully, these research conclusions can be used to further educate college students on cybersecurity and cyber-terrorism. Ultimately, the researchers hope to get all students at Purdue University on the same page when it comes to cyber threats, and with this, the researchers hope to eliminate harmful misconceptions about cybersecurity.

References

Aslanni, A., White, C., & Ettkin, L. (2013). Viewing cybersecurity as a public good: The role of government, businesses, and individuals. Legal, Ethical, and Regulatory Issues 16, pp 7-14. Retrieved December 6, 2021 from goo.gl/iYRV55

Holt, T. J., & Kilger, M. (2012). Examining willingness to attack critical infrastructure online and offline. *Crime & Delinquency 58* (5), 798-822, doi: 10.1177/0011128712452963.

Kenney, M. (2015). Cyber-terrorism in a post-stuxnet world. *Orbis 59* (1), 111-128. doi: 10.1016/j.orbis.2014.11.009

Larson, S., & Pagliery, J. (2017). Ransomware: a malicious gift that keeps on giving. CNN. Retrieved December 6, 2021 from https://cnn.it/2lGFZjh

Luker, M., & Petersen, R. (2003). Computer and network security in higher education. San Francisco, California: Jossey-Bass, ISBN13: 9780787966669.

O'Brien S. (2016). Widespread cyber-attack takes down sites worldwide. CNN. Retrieved December 6, 2021 from http://money.cnn.com/2016/10/21/technology/ddos-attack-popular-sites/index.html

Powlowski, S. & Jung, Y. (2015). Social representations of cybersecurity by university students and implications for instructional design. *Information Systems Education 26*, pp 281-294, url: https://aisel.aisnet.org/jise/vol26/iss4/3