Improving Cybersecurity Awareness in Low-Income Students

Primary Investigator: Belissa Baez

March 24, 2021

Abstract

Cybersecurity awareness can range from understanding how to write a strong password to knowing which Ad-Blockers and Antivirus Software to use. However, studies have shown that the low-income population [6] and young teenage students [7] are prone to having lower cybersecurity awareness. Furthermore, due to the COVID-19 pandemic, many people had to go remote for work and classes. For many, this is an unusual territory that they were forced to be on due to the pandemic, according to the annual Cybercrime Report, cybersecurity attacks after COVID-19 have increased five-fold [8]. This is why it is crucial that we intervene to help prevent them from becoming victims of cyber attacks. Previous papers state that some reasons as to why low-income populations struggle to practice safe cybersecurity behavior are because of language barrier, usage of older phones, internet issues and lack of helpful resources [6]. In this paper, we intervene and attempt to tackle the issue of lack of helpful resources by providing additional education as a tool. That is why we developed a series of workshops for low-income teenagers and measured how it impacted their cybersecurity awareness. This paper addresses existing curricula on this issue and on teaching cybersecurity skills to students. Furthermore, this paper outlines and goes into details the experience and process of the 3 step method that was followed to develop the curriculum and deliver the workshops. In addition, this paper talks about who and why the students we used for our study were chosen. And analyzes the results we obtained from the workshops and how it impacted the students cybersecurity awareness. Finally, this paper discusses future work that can be done as an extension of this thesis to help address other factors that are obscure yet relevant to this issue.

Keywords: Cybersecurity Awareness, Low-Income, Likert Scale, RSeBIS Scale, Underserved population, Pre-Survey, Post-Survey, Workshops

Contents

List of Figures

1 Introduction

Underserved populations are at a disadvantage with regards to experiencing a safe web browsing experience. Such issue stems from the fact that they don't have the appropriate resources to be aware of how to stay safe. While this issue has yet to be entirely solved, one can begin by providing education as a tool for these populations on the concept that is cybersecurity.

1.1 Importance and Relevance

In this research, the question is "How to improve cybersecurity awareness in low-income students?" This question, will guide us to our first task and goal which is to focus on the underserved student population. Then we will proceed to determine how the current cybersecurity curriculum (if available at their school) puts them at an advantage or disadvantage in regards to their cybersecurity awareness. In addition, the second goal that will help with the research question is, including an interactive aspect when I teach the students. With guidance of existing cybersecurity curriculums, I will be able to edit and modify so that I can deliver concise yet informative workshops to my students. Through these actions, I will be able to contribute to the belief that one deserves to be protected and aware of dangers that lurk on the world wide web, despite their income status.

Gaining insight into this research and actually taking the time to gain knowledge from it will allow the reader to understand how to better educate underserved student populations. A solution can be incorporating better resources about cybersecurity in the curriculum taught in schools. This way students will be exposed to these measures at an earlier age which will allow them to keep on exercising such habits for the rest of their web browsing lives.

The importance of this study lies in the fact that low income people are more prone to being victims of cyber scams, as can be seen in Figure 1. It can be seen that 24 percent of the undeserved responded that they have been a victim of cyberscam, which is more than the control group which was 15 percent [6]. While there was an attempt to match income level of underserved respondents and control group, only 20 percent of the comparison group had respondents with an income of less than 25,000 US dollars which is less than the 45 percent involved in the underserved group. Overall, the underserved group was less prepared which led them to have a higher chance of an unsafe experience online.

1.2 Reasons why underserved populations are more likely to be victims of online scams

Some reasons as to why underserved residents struggle to practice safe cybersecurity skills is because for many, English is their second language. Trying to find cybersecurity resources in their native language becomes an issue. Also, another reason that adds to this disadvantage is that underserved populations tend to use older smartphones that are not supported by software makers. This means that their smartphones are not guaranteed to receive the new security and software updates. Finally, another reason is because they are less likely to access online services that aid with online protection [6]. While these hypotheses provide some reasons behind the disadvantage, it is still a challenge to conjugate a concrete reason since there is not enough study done that explores cybersecurity outcomes for low socioeconomic individuals [6].

1.3 Reasons why additional education is still helpful

In this study, the participants were 65 years of age or older[6]. And in the study conducted by Egelman,S et al. [2], the participants age range was from 18-69. This shows us that there is not much of a focus on people younger than 18 years. This is an issue because teen students are part of the age group where education is compulsory [1] and depending on their school, they spend time using many modes of learning such as technology, yet they are not being included in these studies. In addition, because of the COVID-19 pandemic, many of the classes and activities had to be moved to remote status. This means that students are one of the groups who are spending a lot of time online due to their academics. Now is the optimal time to intervene and teach these young students cybersecurity principles since they are online for a majority of the time.

That is why additional education would benefit them since it is a resource that quickly addresses the lack of cybersecurity awareness. Especially since there are many modes of teaching online such as Zoom, which makes the increases the accessibility factor to reach the students in a safe way. Also, they have the time and designated environment to incorporate these skills since the pandemic has caused them to depend on technology even more.

1.4 Project Overview

In an attempt to address the issue of lack of helpful resources about cybersecurity and to answer the question, "How can we improve cybersecurity awareness in low-income students?" I decided to provide additional education by developing my own workshop sessions for low-income students. This paper outlines the 3 main steps that were taken to execute these workshop sessions, which were surveying the teacher,

developing curriculum and delivering the workshops. Also, I discuss what group of students I ended up working with and why I chose them. It also discusses the students knowledge on cybersecurity before and after the workshops, and the overall results that these workshop sessions had on the students cybersecurity awareness. These results were obtained by administering a pre- and post- survey.

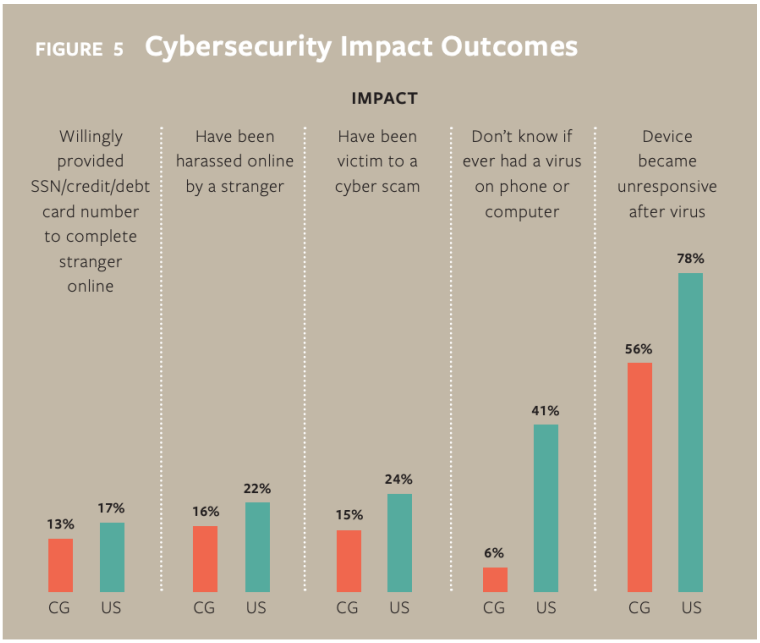


Figure 1: Comparison between a control group and under served group to identify the negative impacts faced due to cybersecurity unpreparedness

2 Related Works

2.1 Existing Curricula

There are studies that have been done where there is a structured cybersecurity curriculum already being taught to High School students [3]. These studies range from a capstone project to incorporating actual video games to teach the cybersecurity principles [5]. With these lesson plans and interactive teaching, there have been attempts to create relevant and efficient methods to grade the students' understanding of taught concepts [9]. It makes sense that when grading students work, it is interactive and relevant to what you have taught them. In other words, modifications have to be made to the grading rubric so that the students are aware on what they are being graded and it is a transparent process for both the student and the teacher.

Furthermore, video games have been used to teach cybersecurity principles. However, in this study, the results revealed that the male students enjoyed the video games more than the female students [3]. This is one of the reasons why in this research, video games will not be used. This research attempts to cater to both females and male students.

Finally, the video game study has some topics this research will attempt to educate the students about such as identifying phishing emails and tailgating. While these topics will not be implemented through video games, this project will still incorporate them. The main goal as stated before is to teach these students ways that they can stay safe online and with the guidance of such existing curriculum. In this section I will review prior work done in cybersecurity awareness, cybersecurity behavior and teaching cybersecurity skills.

2.2 Prior research on differences in cybersecurity behavior between different demographic groups

In the study, "Self-Confidence Trumps Knowledge: A cross-cultural study of security behavior", the authors ran an online study to see how culture affects online security behavior. They analyzed over 3,500 responses using linear regression. They found that income does have a large effect on security behavior. Participants with an annual income of at least $60k$ or more in the US had a higher score on security proficiency as compared to the participants with a lower income (less than $60k$). French participants were more secure online as compared to people from Asian countries. [2] As we can see from both of these studies, there is a relationship between income and the awareness of confidence that people possess when it comes to practicing safe online behavior. In this study, the groups that are at a disadvantage are low-income people, hence why this research focuses on working with low-income students. The study mentioned before, described the connection between low-income people and their behavior when it comes to being secure online. This next study, focuses on improving this issue where low-income people are prone to cybersecurity attacks.

In the study, "Improving cybersecurity Awareness in underserved populations" there were two groups that were studied. In the underserved group, the average income was $35k$ or less. When this group was compared to a comparison group, the underserved group was prone to experiencing cyber scams. In the comparison group, 15 percent were victims, which is lower than the 24 percent in the under served group is lower. In addition, when asked if they knew if they had a virus on their phones or computers, 8 percent of the comparison group said they did not know while 41 percent of the underserved group said the

same [6]. One can see that the underserved group is at a disadvantage when compared to the comparison group. Furthermore, this report discusses different ways that this issue of cybersecurity awareness can be improved. One way is for city leaders to study their own populations cybersecurity awareness and help provide targeted training (I plan on teaching which is similar to targeted training). Another way to help is to partner with private sectors so that state and federal programs can help underserved residents with resources such as advice websites and public awareness campaigns. [6]

2.3 Prior work on teaching cybersecurity skills

There exists prior research that discusses the teaching of cybersecurity skills to students. One way that these skills have been introduced is via video games. In this study, they created a game called Cyber Defense Tower where the students had to protect their servers from incoming cyber-attacks. The topics taught via this virtual 3d game were "Piggybacking, tailgating." These are the same topics I plan on incorporating into my lesson plan as well. In addition, many underserved students such as African-Americans and Hispanics attended the GenCyber Summer Camp at Purdue University. A "total of 181 High School students attended the summer camps with 51.3 percent being underrepresented African American and Hispanic students. The male to female ratio was 2.12 to 1". [3] This is beneficial to supporting the purpose and importance of my project since there have been attempts to educate underrepresented youth about cybersecurity.

Furthermore, another paper focused on using the cat and mouse online game to teach basic computational skills. It helped beginners understand the concepts better since they were able to visually see the concept. Here they used Roboscape to incorporate robotics into teaching cybersecurity principles. The harder the levels got, "this culminated in a final challenge that required implementing defensive measures such as encryption, secure key exchange, and sequence numbers to prevent cyber attacks during robot operations." So, the levels allowed for the students to show progress in their understanding, since they had to incorporate more skills as the levels got harder. Furthermore, a pre-survey question they asked was if the students had any prior CS knowledge. This is helpful to know so that the educator can identify how much time should be spent on certain topics.

Their grades were higher if they used more loops, because the educators saw the students were challenging themselves. This makes sense because if the student incorporates more of what they have learned, then the educator will see that they are attempting to grasp better knowledge of the content and that can only be done by practicing the learned skills. They quizzed students on cybersecurity questions that involved analyzing algorithms and asking questions such as "what makes cryptographic algorithms secure". They were

able to monitor the progress of the students by asking similar questions in a post survey. [9]. Also, there has been a capstone project done where a group of undergraduate students as a capstone project created a software called Vulnerable Web Server. It has packaged materials for computer security that High School and college educators can use. Powerpoints, youtube videos, lesson plans on cybersecurity. Anyone who wants to teach cybersecurity measures to a non CS person can use this [3].

3 Method

The execution of this project was divided into three main parts, which are surveying the teachers, developing curriculum and delivering the workshops. I developed a series of three workshops targeting Middle School and High School students and tested their cybersecurity awareness with a group of students in that age range.

3.1 Survey the Teachers

3.1.1 Surveying the Teachers: The Process of getting an interviewee

The time allocation designated for this part of the project was two weeks during winter term of 2021. In the first week, I sent out various emails to different local High School IT and Computer Science teachers. The reason I sent it to these teachers was because they know more about the Computer Science and cybersecurity curriculum since this is the focus of their teaching. Such High Schools involved, Schenectady High School Niskayuna High School, Mohonasen High School, Guilderland High School, Scotia-Glenville High School, Schalmont High School, Colonie Central High School, Shaker High School, Bethlehem High School, Tech Valley HS - Albany, Albany High School. However, only one teacher got back to me. Brian Rozmierski, an IT teacher, from Tech Valley High reached back. Since my project had a strict deadline I had to adhere to, it was decided that one teacher would suffice for an interview following the second week. The interview was scheduled during the second week of the term, via Zoom at the teacher's convenience.

3.1.2 Surveying the Teachers: The Interview Questions

During the interview, the questions that I asked Mr. Rozmierski were:

- How much time is spent on teaching cybersecurity?
- Is there a topic in cybersecurity that you feel students struggle with the most?

- Does the student's socioeconomic status affect their ability to practice safe online cybersecurity behaviors?
- Do you feel more cybersecurity content is missing from the tech/CS curriculum at HS? Why do you feel this is?
- If you could, what would you include in your cybersecurity curriculum but cannot due to low resources or time constraints?
- What kind of topics would you recommend I cover for cybersecurity?
- Advice on how to assess the STEP students?

3.1.3 Surveying the Teachers: The Answers

- His response to the first question was, not much time is spent on cybersecurity. It is not a big part of the Computer Science curriculum.
- A challenging topic the students encounter is input sanitization and checking inputs before processing them. In addition, another struggle is having concise code, and understanding an algorithms complexity.
- The biggest issue with disadvantaged students from a socioeconomic perspective is that cybersecurity material is hard to grasp because they don't have exposure. They don't have exposure or background experience for it. As a teacher, you can model and teach the concepts, but the hardest thing is making sure the student is able to practice these skills outside of class, because you can't really control that aspect. Access to tech is the common denominator that exasperates all the other.
- If it was required by the state curriculum, he would not mind teaching cybersecurity skills. However, the state mandated curriculum is tough and it also depends on the school. For his school specifically, they teach technology on a daily basis which means they have a different model since everything they do is digital. However, the only cybersecurity aspect they mainly cover is during freshman seminar on appropriate things to download.
- If he could include anything in the cybersecurity curriculum, he would include the concept of privacy as it pertains to security. In addition, he would also focus on the buy in and engagement aspect since that is the hardest part. In addition, finding tools for engagement so that the students can understand the concept better.

- He suggested I talk about privacy to the students. Also, to talk about malware and persistent threats. I should use images to help the students visualize and understand the concept better. Furthermore, I can give expose them by giving an example such as the Nigerian Prince Scam email so that they understand that these emails are real threats and dangerous. I should also make sure that I keep the topics simple so that the progression of cybersecurity topics introduced, run and connect smoothly when presented.

- These workshops should be fun because they are not an actual academic course. He suggested I gamify the assessments such as using a Kahoot. Also, to keep the workshops fun and light, I should not include tests, instead I should use a pre and post survey to test the students progress. Furthermore, my workshops should have visuals such as videos and the activities should be paired so that the students can discuss amongst themselves.

3.1.4 Surveying the Teachers: Take Aways

I wanted to interview a teacher from High School because they have experience with teaching. I was going to do the same which is why it made sense that I received advice from someone with experience. In addition, the content that I taught the students came from majority of this interview. I wanted to teach them something that he believed was not taught enough due to time and State restrictions. In regards to content, he said to talk about privacy issues and scams such as the Nigerian Prince Email. In addition, the assessments should be engaging since this is not an actual a course, I am not required to have tests.

3.2 Developing the Curriculum-The topics

Based off of the interview with the teacher and reading papers on teaching K-12 computing, I decided to create a series of three workshops. The topics I decided to include were based off of the teacher's recommendations and from the papers I read. In the video game study, they focused on tailgating and phishing, so I decided to also focus on those same topics. [3]

The final topics that were included in the workshop sessions were:

- Session 1
  - Phishing Emails
  - Spam Emails
  - Nigerian Prince Scam Email
- Session 2

  - Tailgating
  - Piggybacking
  - Creating Strong Passwords

- Session 3
  - Malvertising
  - Ad-Blockers
  - Antivirus-Software

These topics built off of each other. In session 1, the focus was on identifying dangerous emails, which is why I showed them three different examples of emails. For session 2, the focus was on securing your devices. I started with introducing the ideas of tailgating and piggybacking so that they can see why it is important to log out when using a public computer. Also, identifying when someone else is trying to gain access. After these concepts were introduced, they now had an idea why it was important to create a strong passwords, so that these social engineering attacks can be prevented. Finally for session 3, I started with introducing what malvertising was. To solve this issue, I then talk about Ad-Blockers which is one solution to this. And a bigger solution wold be antivirus software which I ended my session with.

3.2.1 Developing the Curriculum-The Activities

The activities for each session were based off of the workshop and topics introduced for that day. For the first session, the activity that was planned was to write your own example of a dangerous email. Studies have shown that students only learn 20 percent of what they hear and read, but learn 90 percent of what they practice[4] which is why these activities were designed to be interactive. So that they can actually retain the content.

For the second session, the activity that was planned was using passwordmeter.com to test good and bad passwords. This would help them understand what makes a password weak or strong. They did this by being in two breakout rooms and writing their findings on a shared google doc so that their ideas could be monitored by me.

For the last session, the activity planned was a Kahoot. The purpose of this Kahoot was to have gamefied summary of all of the topics that we went over for all of the sessions.

4 Deliver the Workshops-Format and Experience

Before I discuss in detail the implementation of these workshops, I should state that the students that I ended up working with were STEP students who are part of the STEP program. The STEP program helps underserved students for entry to STEM college programs. These students fit my criteria for my project since they are low-income and are teenager students in Middle School and High School. Union already has an established relationship with STEP, which is why asking for permission from the Kenny Center to work with them, was not a challenge. After I presented my project to the the Interim Director of the STEP program, Janet Sweeney, I received approval and we advertised my workshops to the students to recruit them. In order to get them more motivated to join, they were offered an incentive, which was free pizza delivered to their homes if they came to all three sessions.

Also, due to COVID-19, the workshop sessions were all done virtual via Zoom. They took place every Friday during weeks 6-8 of the term from 5-6pm.

The actual lesson plans were organized into three different sets of Google Slides, 1 set for each workshop. This was done to provide an easier visual experience for the students and myself. The slides were easier to go through since I just had to share my screen via Zoom.

Overall, the experience of teaching was fun and comfortable. When teaching, I would ask the students to either unmute themselves or write in the chat their responses or questions they had for me. It worked for most of the time. When I needed an answer, someone would respond to me. Only two people had their cameras on for all three sessions. I did not enforce cameras on because the High School teacher I interviewed told me to be aware that some students have situation going at home, so I had to be understanding. Regardless of this, all of the students still participated.

4.1 Deliver the Workshops-The students responses to my questions

Before I introduced a definition for a topic, I asked the students for their own definitions before I gave them the actual definitions.

Here are some examples of their responses for the question I asked:

What are Phishing Emails and Spam Emails?

- Unsafe emails
- Malicious email
- Email with a suspicious link

They were aware of the idea behind dangerous emails and were able to give answers that were close to the actual definition.

For the second session, I asked for a their own interpretation of what tailgating and piggybacking meant. They response were:

- Taking stuff that belongs to other people like credit cards
- Stalking someone on social media

These answers were not close to the actual definitions, which makes sense since in the survey, as can be seen in Figure 9(a), they stated that they were not as familiar with these terms.

In addition, before I showed them various ways to prevent piggybacking and tailgating attacks, I showed them a video that explained these topics in more details. After that I proceeded to ask them, What were some ways they can think of to prevent such attacks? These were their responses:

- Using password for you wifi to prevent piggybacking
- Log off every time you are done using a public computer
- Having security awareness
- Installing a password on your phone so you and family can access it
- Confronting people who enter without a adage

These responses were similar to the ways in the video. It makes sense that they would mention these ways since the video stated these solutions.

For my final session, I asked them what did they think malvertising meant.

Their responses were:

- Advertising malware
- Using ads to spread malware
- Ads that adds that have viruses encoded in them

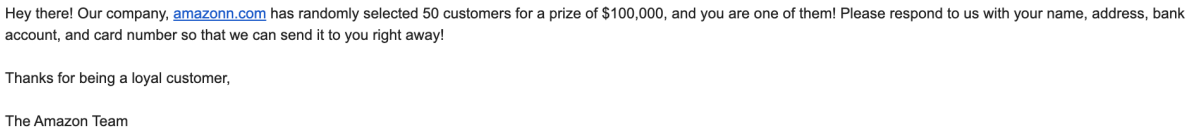
I later asked them, what were some ways they can think of to prevent malvertising? They responded:

- Report it, report ads on Google
- Use an ad blocker
- Using a malware blocker

Their responses showed that they were aware of different solutions.

4.2 Deliver the Workshops-Their responses for activities

Since, the activities were meant to be engaging and interactive, the students were able to provide some work right away. For the first session, I asked them to write their own example of a dangerous email (as seen in Figure 2) and send it to me. Below are some of their examples.


Hey there! Our company, amazonn.com has randomly selected 50 customers for a prize of $100,000, and you are one of them! Please respond to us with your name, address, bank account, and card number so that we can send it to you right away!

Thanks for being a loyal customer,

The Amazon Team

Figure 2: Sample email from a student for the first session activity

For the second session, I asked the students to write in a Google Document different types of passwords that were either good or bad. In Figure 3, we can see the different types of passwords they wrote.

Prompt:

In breakout rooms, for 10-15 minutes, play with passwordmeter to create some good and bad passwords. Share and write in the google docs, what was it that made your passwords good and what made it bad. Add any other observations you noticed !

http://www.passwordmeter.com/

Breakout room 1

- **AuI!3TMu?*N5**
- **Uthase!6.#%^**
- **(!%_6tK;xpsW*}:$**
- **Good passwords used symbols**
- **#:H-uFn{3ENbC4=5**

Good passwords seem to have diversity in characters, complexity, and randomness that have relevance to nothing. Bad passwords are short and too predictable(leaving you susceptible to brute force attacks). A password made up of a bunch of random characters is the least thing anyone would expect. Weak passwords contain entire words.

Breakout room 2

- **Bad passwords have things that are personal**
- **Good passwords have capital and lowercase letters**
- **Good passwords have 15 characters**
- **Good passwords have a mix of symbols and numbers**
- **qAb6&$05pOT@*!#**
- **Lg2103$@**

Figure 3: Password activity for second session

4.3 Deliver the Workshops-My Experience for Each Session

First Session

This section describes my detailed authentic and informal experience with the students. It's representative of a diary for my experience for each of the workshop sessions.

I began with asking them to fill out my form. Here it was quiet since it did have a couple of questions, but I wanted them to answer truthfully. Then I asked them to introduce themselves. I started with introducing myself so that they can have a couple of seconds to think about what to say. Then I asked them to unmute their microphones when they introduced themselves. I asked why they were interested in these sessions and majority said because they want to be more aware on how they can practice safe cybersecurity measures. And to help me with my thesis!

After the introductions, I told them we would be covering phishing, spam and Nigerian Prince Scam emails. Before I spoke further, I wanted to understand what did they already know. That is why I asked them what do they think of when they hear these terms. Majority wrote in the chat. They said things such as, unsafe emails, malicious email, and emails with a suspicious link. Then I introduced the definition of phishing. Someone asked if they can take notes and I said yes!

Then I proceeded to show them the example of the emails. For each of them I asked what do you guys see that makes these emails phishing. They were able to spot the difference between them and would write it in the chat.

Then I introduced them the definition and examples of spam email. I proceeded to ask what made these emails Spam. They said because it is Mark Zuckerberg and he would not give us free money like that. And the link to his bio is very suspicious. And for the next one they said that it is in another language. Finally, for the Nigerian Scam email they saw how private information is trying to be taken from them.

I then had them write their emails and send them to me. When we read them out loud they would respond in the chat. Many of them had humorous comments such as "Belissa you should pay your taxes or else they'll take your puppies!" and I interacted as well saying "Yes lol". I tried interacting with them in this way because I too am young and they were having fun with identifying these emails. I asked them what they think the emails were and they'd respond in the chat and the person who originally wrote the email would identify it. I'd ask is that correct, to the person who wrote it and they would confirm in the chat.

Overall even though the majority had the cameras off, they interacted with me in the chat. And the two who did have the cameras on would umnute themselves or give me hand signals to know they were actively listening. When I would call on someone with their cameras off, they'd respond in the chat.

Second Session

I began by asking them an icebreaker question. They answered by unmuting themselves or writing it in the chat. Then I told them that today we would be talking about securing your devices and I asked them what do they think tailgating and piggybacking means. They said they thought it meant taking stuff that belongs to other people like credit cards and stalking someone on social media.

Then I proceeded to tell them the actual definitions and showed them some videos going into more details about piggybacking and tailgating.

I then proceeded to ask them about how could you prevent such attacks. They said: using passwords for your wifi to prevent piggybacking, having security awareness and confronting who enters in an authorized area without a badge.

After showing them the different ways they can prevent such attacks and how to make a strong password, I had them play with password meter. To see what they think would make a good password good and what makes a bad password a bad one. I divided them into two breakout groups.

Final Session For my final session, it was short and the students were respectful and spoke up when needed. We played Kahoot and I administered the post-survey after the Kahoot so that they could remember our lessons before the post-survey.

5 Results

5.1 Student Demographics

The gender distribution was 4 students were female and 3 were male . The age range was from 13-17 years old. The schools the students attended, were near the local Albany area as can be seen in Figure 4.

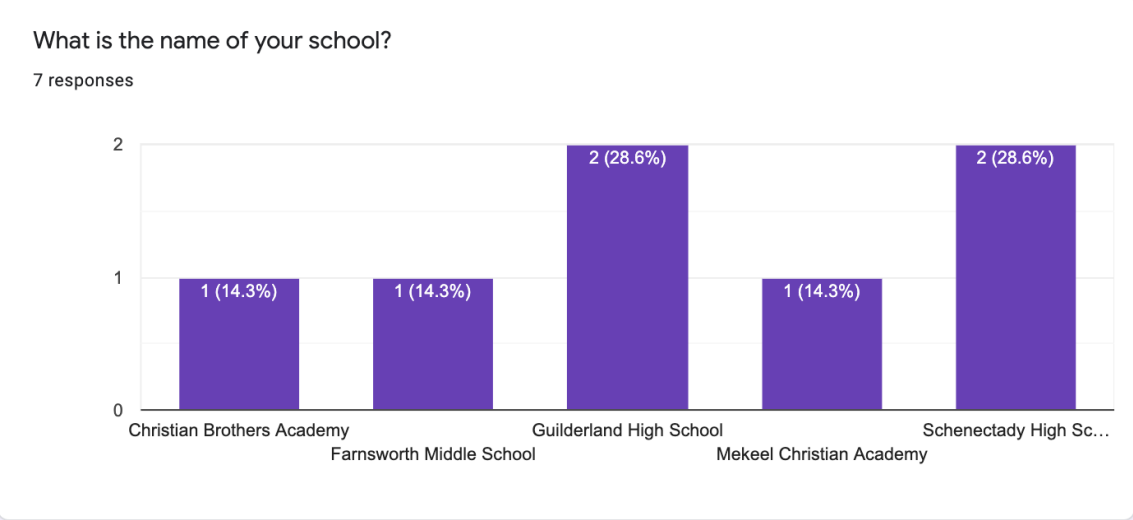


Figure 4: Schools the students attend

5.2 Results-Pre-Survey

For my own survey, I borrowed and modeled the rest of my questions based on the RSeBIS scale. I did some alterations to my questions, where the Likert-Scale now ranges from 1-5 where 1 is Strongly Disagree and 5 is Strongly Agree. Also, it is important to declare that the pre-survey was administered before the first workshop began in order to get an idea of how much the students already knew. And the post-survey was administered after the last session, to see the students evolution in their confidence level in regards to cybersecurity awareness. Below are the questions I actually included from the RSeBIS scale and the rest of my survey questions.

These are the questions from the RSeBIS scale that I actually asked in the pre- and post- survey:

- I use a passcode to unlock my phone
- I include special characters in my passcode even when I am not prompted to do so
- I know how to create a strong password.
- When I get a notification to install a software update, I do it.
- Before I submit information to a website, I check to see that there is a lock icon on the URL.
- I have an anti-virus software installed and I verify that my anti-virus software is up to date.
- I have different passwords for different accounts.

These are the rest of my survey questions for pre-survey:

- I know what is a password manager and how to use one.
- I know what an antivirus software is.
- I know how to get rid of a virus on my computer (using ad blockers, antivirus software and etc.)
- I know how to identify when an email is legit or not.
- I am aware of the term phishing emails and can identify what they are.
- I know what piggybacking means.
- I know what tailgating means.
- I know of some ways to prevent tailgating and piggybacking attacks.
- I know how to identify a spam email.
- I know what the Nigerian Prince Scam email is.
- I feel safe when I am exploring the internet and can apply safe cybersecurity measures.
- I know what malvertising is.
- I know what an Ad blocker is and how to install it.
- I feel comfortable using an Ad blocker for malvertising.

For majority of the the pre-survey results, the students were in the neutral zone and the Strongly Disagree zone. This can be seen in Figure 7(a) where they were asked about preventing piggybacking and tailgating attacks and in Figure 8(a) where the students were asked if they felt comfortable identifying phishing emails.

Another example can be seen, when the students were asked about piggybacking, in Figure 9(a) where majority of the students fall in the Strongly Disagree area. Furthermore, a large portion of the students strongly disagreed that they knew how to use a password manager as seen in Figure 10(a).

While there were instances of Strongly Disagree, there were also few instances were students felt comfortable. Such question was when I asked them if they had a password on their phones, all of the students strongly agreed with the statement as can be seen Figure 6.

Overall, despite the students already executing some safe cybersecurity behavior to a certain extent, they all strongly agreed that they could improve their cybersecurity awareness, as can be seen in Figure 5.

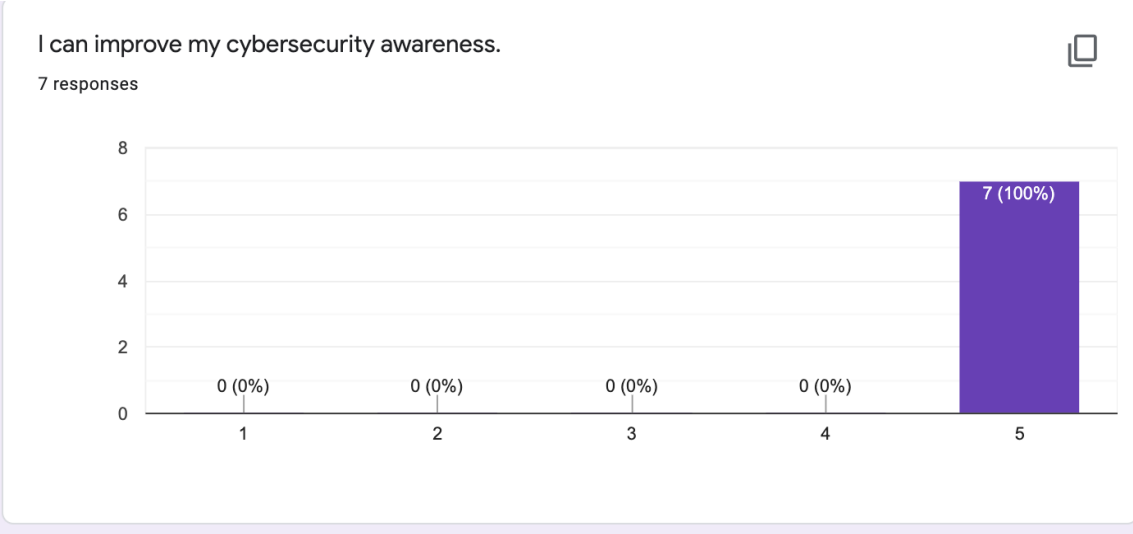


Figure 5: Pre-Survey Response for increasing cybersecurity awareness

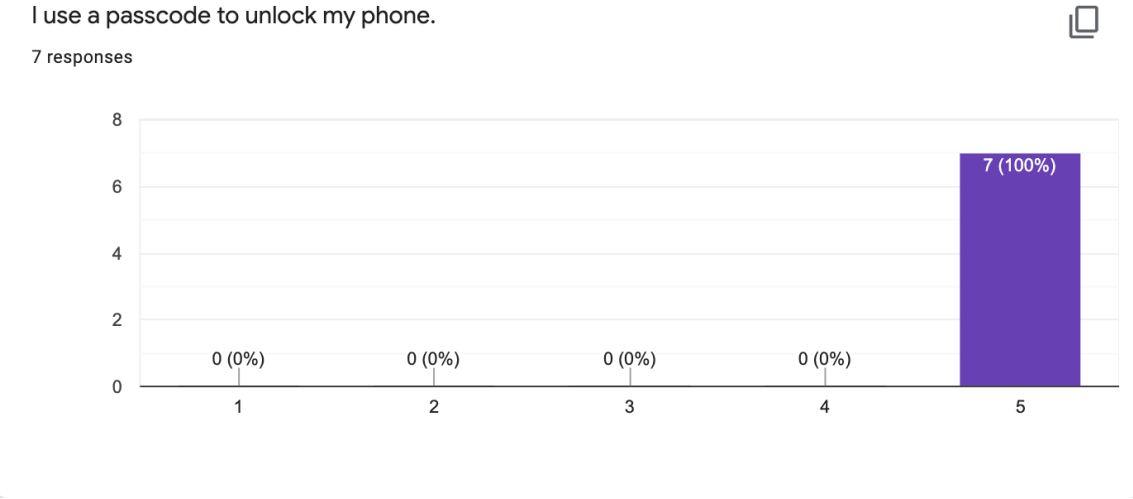


Figure 6: Pre-Survey Response From RSeBIS Scale

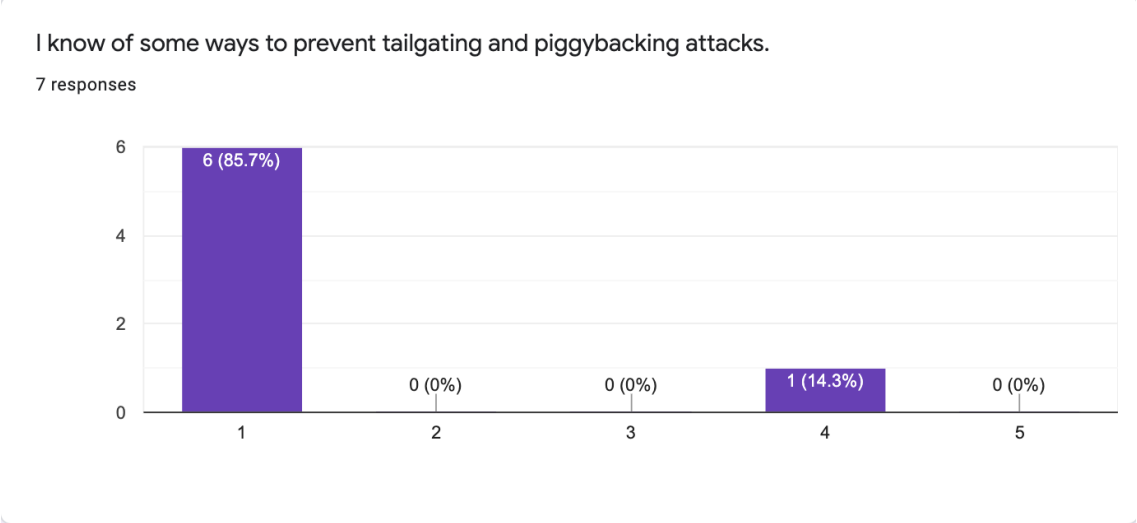
5.3 Results-Post-Survey

For my post-survey, the questions were the same as the pre-survey questions, but I added some extra reflection questions which are stated below.

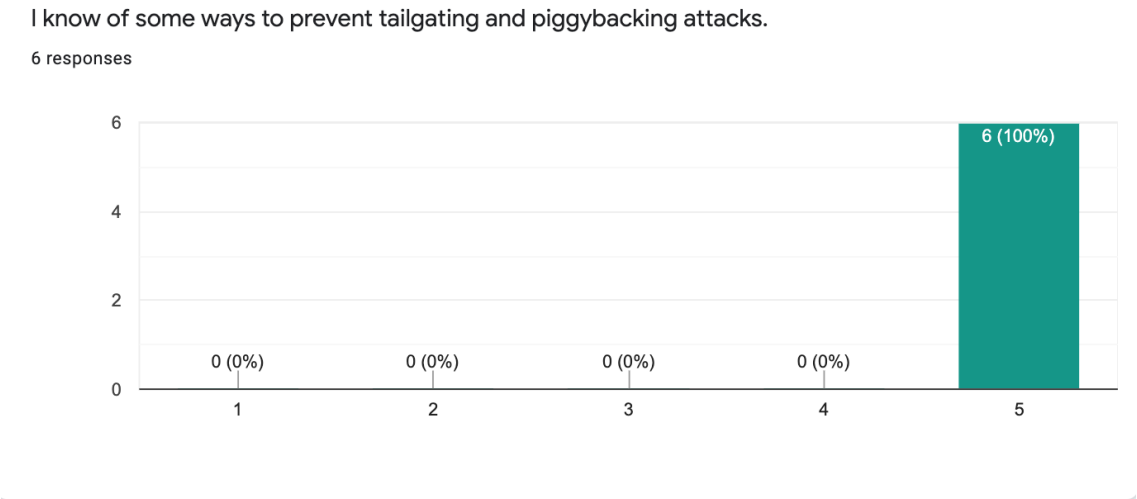
Extra reflection questions added to post-survey:

- In your own words, what do you think cybersecurity means now?
- In your own words, what did you learn from these workshops?
- In your own words, do you feel more prepared to use these new tools to explore the web in a more safer way?
- I felt these workshops were helpful in increasing my cybersecurity awareness.
- Anything else you'd like to say? Feel free to write it here

For all of the post-survey results, all the students were now in the Agree and Strongly Agree zone. One example of this is in Figure 7(b), we can see how all of the students are more comfortable with identifying ways to prevent piggybacking and tailgating attacks. Another example can be seen in Figure 9(b) where all of the students Strongly Agree that they now know what piggybacking means. Also, we can see that all of the students Strongly Agree that they know what a password manager is, as seen in Figure 10(b). In addition, all of the students strongly agreed that they now know how to identify phishing emails, as seen in Figure 8(b). Furthermore, in Figure 13, we can see that all of the students Strongly Agreed that these workshops were helpful in increasing their cybersecurity awareness.



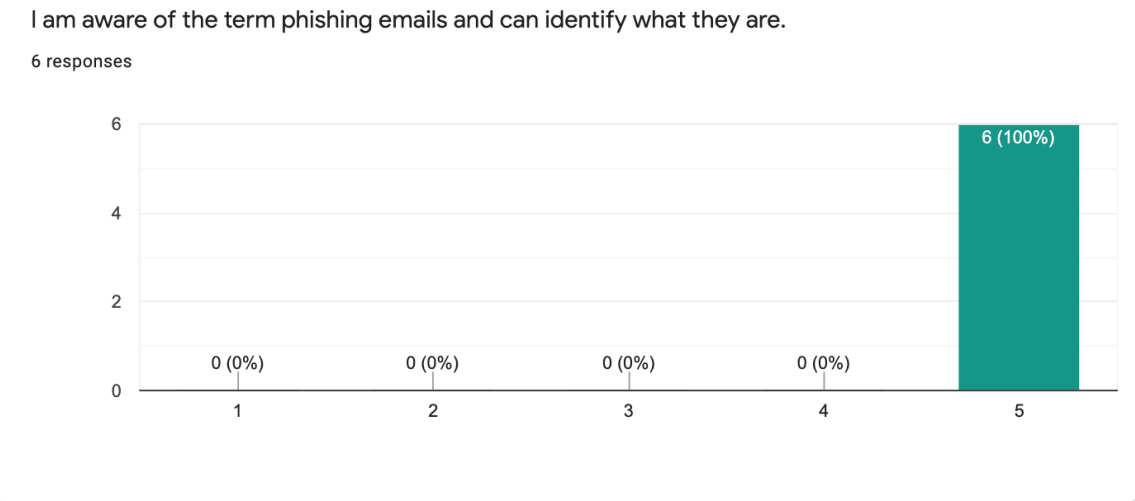
(a) Pre-Survey



(b) Post-Survey

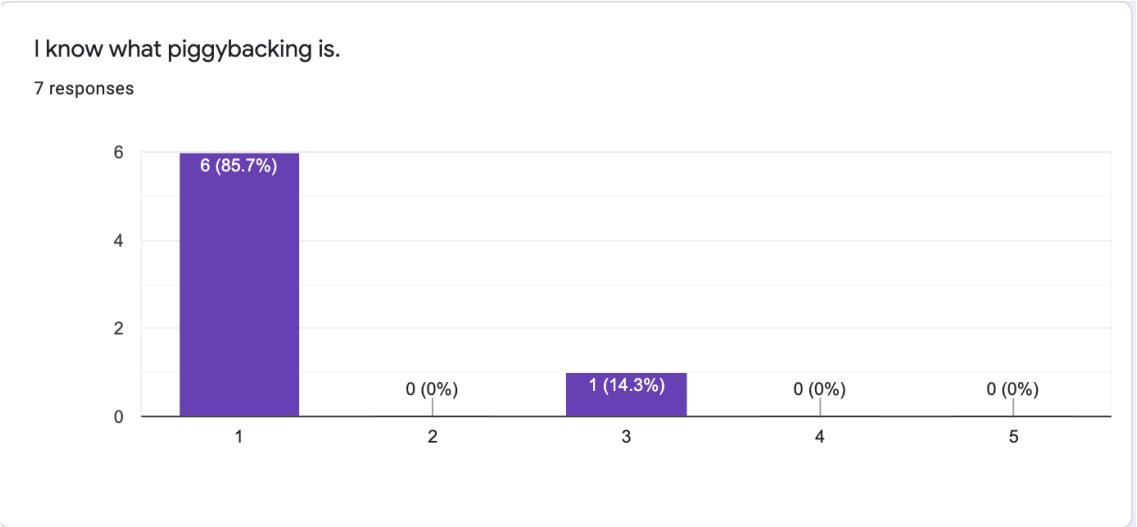
Figure 7: Pre- and post- survey results for identifying ways to prevent tailgating and piggybacking attacks.

(a) Pre-Survey

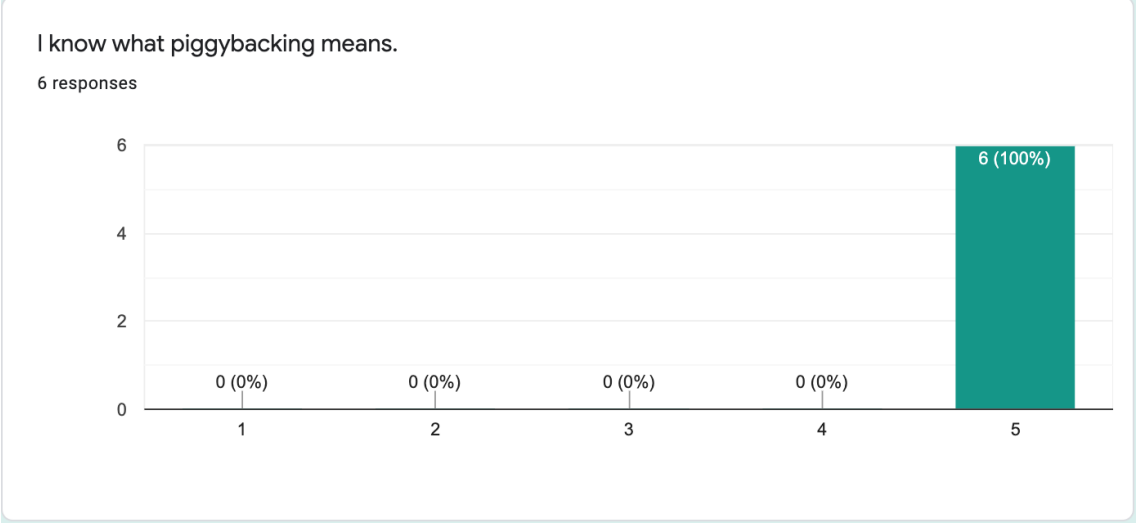


(b) Post-Survey

Figure 8: Pre- and post- survey results for identifying phishing emails.

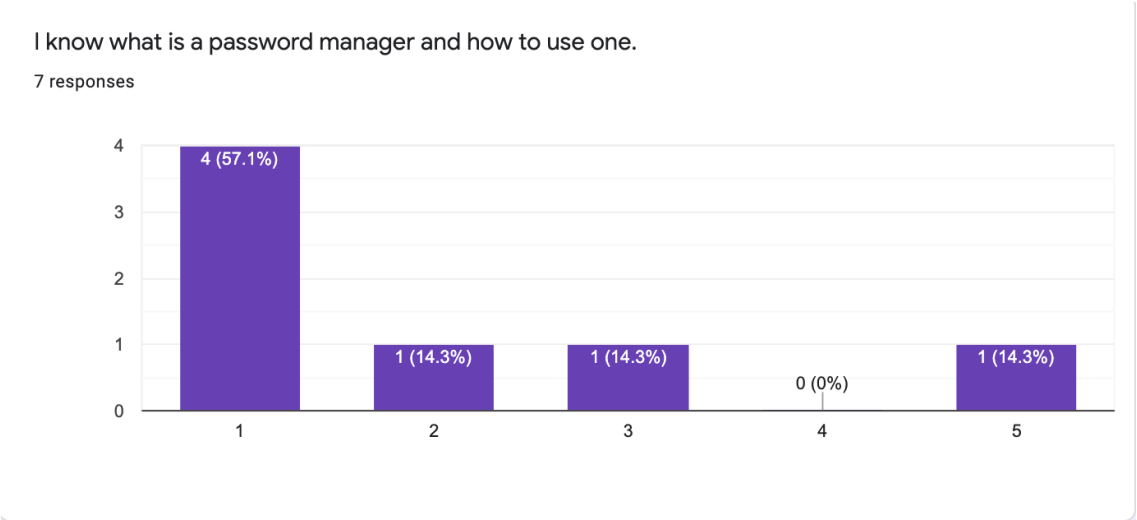


(a) Pre-Survey

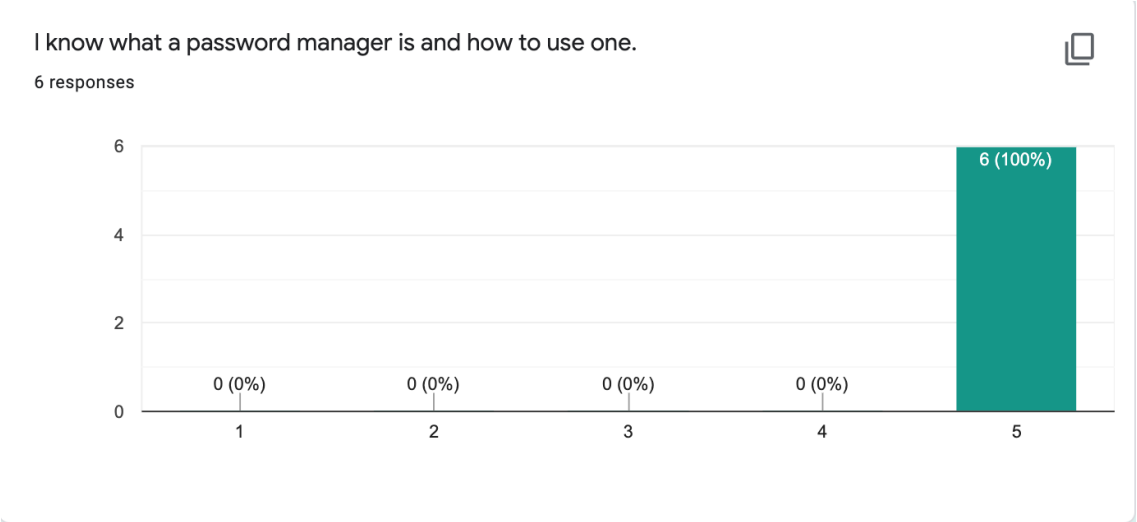


(b) Post-Survey

Figure 9: Pre- and post- survey results for identifying piggybacking.



(a) Pre-Survey



(b) Post-Survey

Figure 10: Pre- and post- survey results for using a password manager.

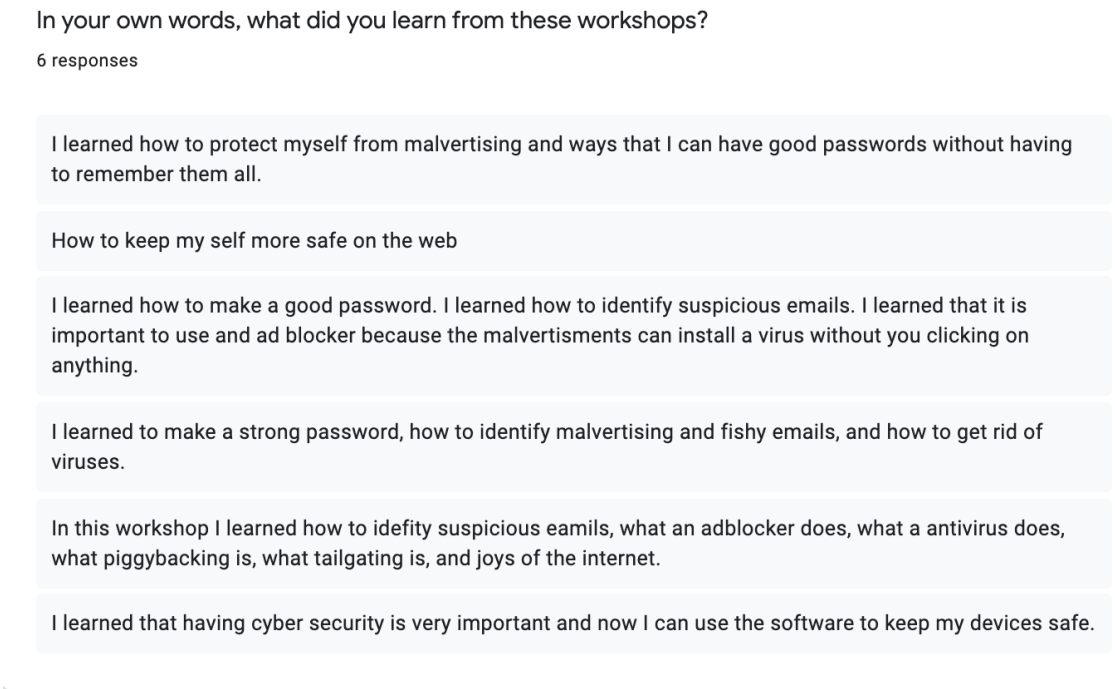


Figure 11: Post-Survey Student Reflection: Take aways from the workshops

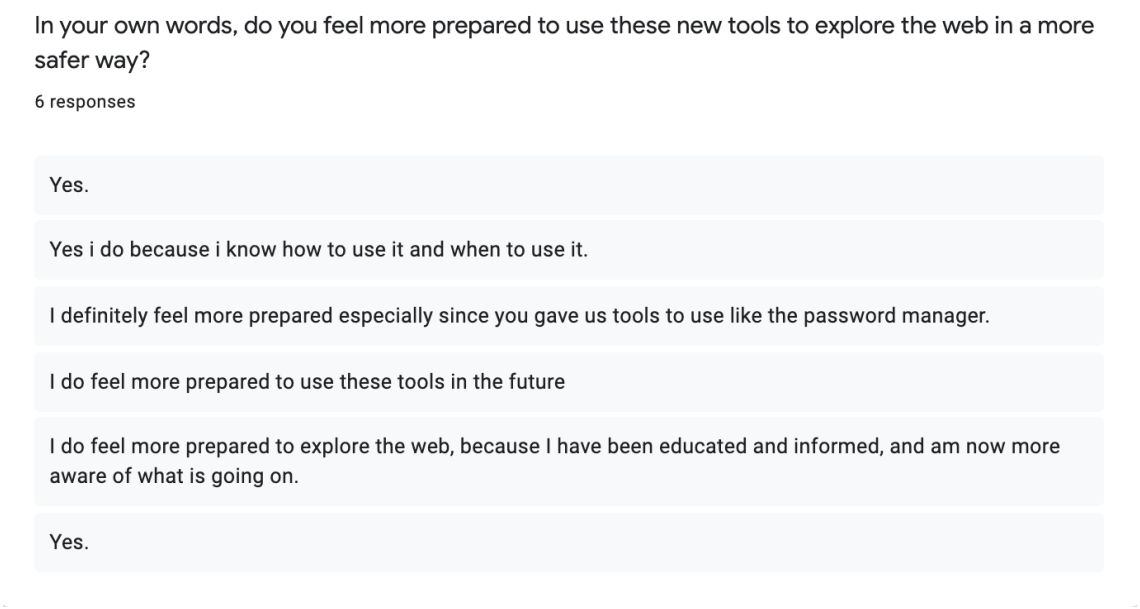


Figure 12: Post-Survey Student Reflection: Preparedness to explore the web

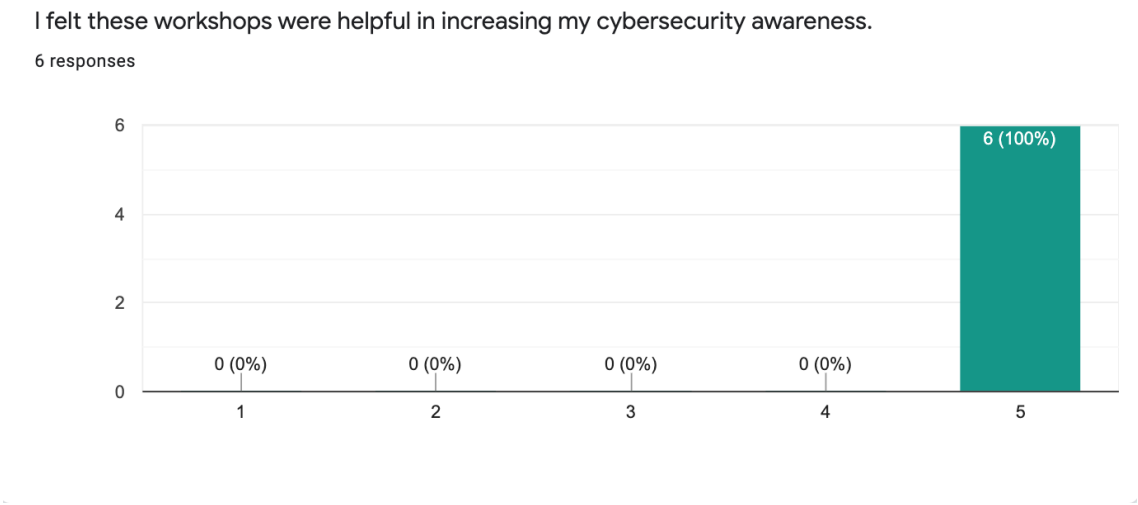


Figure 13: Post-Survey Response

6 Conclusion

To conclude, these workshops, which served as additional education to solve the issue of lack of helpful resources, did help the students increase their cybersecurity awareness.They were indeed helpful in answering the questions of how to improve cybersecurity awareness in low-income students, as our results can show us. Before diving into the post-survey results. I will discuss the pre-survey results in more details. In Figure 5, I asked them if they felt they could improve their cybersecurity awareness. All of them strongly agreed that they could. The reason I asked this question was because I wanted to make sure that the students I was delivering these workshops to, actually had low-cybersecurity awareness, which is what my project was focused on. Also, since I was using the RSeBIS scale as a model, I used some questions from that scale and incorporated it into my own survey. We can see in Figure 6, that all of the students were using a passcode to unlock their phones. This response led me to believe that these students were already practicing some safe cybersecurity behavior on their own, on a device they use frequently, however, as stated before, they agreed they can improve their awareness. Overall, for the pre-survey results, the students were somewhat aware of ways to stay safe on the web, but not enough where it should be.

After the post-survey was administered, the results showed that the students progressed in their awareness. In Figure 8(b) we can see how all of the students agreed that they can now identify phishing emails which is an improvement from the first session where none of the students were in the Strongly Agree area, as can be seen in Figure 8(a). In addition, as can be seen in Figure 9(b), these students are comfortable with the term piggybacking and why this term is relevant to understanding how to prevent attacks. This is a dramatic improvement from session 1, as can be seen in Figure 9(a), where majority of the students were in the Strongly Disagree area and only 1 was in the neutral zone, while none of them were in the Strongly Agree area. Furthermore, there was an improvement with the students ability to identify different ways to prevent tailgating and piggybacking attacks as can be seen in Figure 7(b). Compared to the results from Figure 7(a), the students feel more comfortable tackling this issue now after the workshop. This is a good result to witness since they can now protect themselves from these attacks because they are aware on what this attack is and how this attack can manifest itself.

Overall, the students had a dramatic improvement from the first workshop to the last workshop. Not only did their confidence in identifying cybersecurity terms increase, but as we can see in Figure 10(b), their confidence to understand how to use a security tool such as a password manager, also increased. These workshop sessions were short, but they were enough to provide the students with tools that I provided to them, after the sessions via email, and knowledge from the sessions. They not only learned but also enjoyed

the workshops which was part of my goal. To keep it interactive, but also fun. Their honest responses to the workshop sessions can be seen in Figure 11 and 12. They clearly discuss that they did learn from the workshops and also feel more prepared to explore the web in a safer way.

7 Future Work

Additional work can be done in improving cybersecurity awareness in low-income students. Current papers and studies focus on adults and use games to teach cybsercurity curriculum to High School students. However, there are not much studies done that focus on the socioeconomic aspect of this issue. Future studies have to be done that focus on the participants or students income in addition to their cybersecurity awareness. Specifically, the studies need to recruit a low-income population for their study. Preferably, young people since older people may resort to using less technology, to have more relevant and accurate data, younger populations are preferred. Furthermore, analysis of current cybersecurity curriculum in Middle and High Schools have to be done. Additionally, a study on the State's budget has to be done as well to understand how these budget limitations may affect what actually gets taught in the classroom.

Future work for my thesis would involve having two groups for my study. One group would be the low-income group and the other group would be the high-income group. This way I can focus more on the socioeconmic factor and see which group has a higher and lower cybersecurity awareness based off of their income status.

References

[1] DIFFEY, L., AND STEFFES, S. Age requirements for free and compulsory education. 50-state review. *Education Commission of the States* (2017).

[2] EGELMAN, S., AND PEER, E. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (New York, NY, USA, 2015), CHI '15, Association for Computing Machinery, p. 2873–2882.

[3] ESTES, T., FINOCCHIARO, J., BLAIR, J., ROBISON, J., DALME, J., EMANA, M., JENKINS, L., AND SOBIESK, E. A capstone design project for teaching cybersecurity to non-technical users. In *Proceedings of the 17th Annual Conference on Information Technology Education* (New York, NY, USA, 2016), SIGITE '16, Association for Computing Machinery, p. 142–147.

[4] JIN, G., TU, M., KIM, T.-H., HEFFRON, J., AND WHITE, J. Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn) 12*, 1 (2018), 150–158.

[5] JIN, G., TU, M., KIM, T.-H., HEFFRON, J., AND WHITE, J. Game based cybersecurity training for high school students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (New York, NY, USA, 2018), SIGCSE '18, Association for Computing Machinery, p. 68–73.

[6] SULTAN, A. Improving cybersecurity awareness in underserved populations, 2019. https://cltc.berkeley.edu/wp-content/uploads/2019/04/CLTC$_{U}nderserved_{P}opulations.pdf$.

[7] TIRUMALA, S., VALLURI, M. R., AND BABU, G. A survey on cybersecurity awareness concerns, practices and conceptual measures. In *2019 International Conference on Computer Communication and Informatics (ICCCI)* (2019), IEEE, pp. 1–6.

[8] WILLIAMS, C. M., CHATURVEDI, R., AND CHAKRAVARTHY, K. Cybersecurity risks in a pandemic. *Journal of Medical Internet Research 22*, 9 (2020), e23692.

[9] YETT, B., HUTCHINS, N., STEIN, G., ZARE, H., SNYDER, C., BISWAS, G., METELKO, M., AND LÉDECZI, A. A hands-on cybersecurity curriculum using a robotics platform. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (New York, NY, USA, 2020), SIGCSE '20, Association for Computing Machinery, p. 1040–1046.