California State University, San Bernardino

CSUSB ScholarWorks

Electronic Theses, Projects, and Dissertations

Office of Graduate Studies

6-2019

SECURITY PRACTICES: KEEPING INDIVIDUALS SAFE AND AWARE IN THE CYBER WORLD

Annie Respicio

Recommended Citation

Respicio, Annie, "SECURITY PRACTICES: KEEPING INDIVIDUALS SAFE AND AWARE IN THE CYBER WORLD" (2019). *Electronic Theses, Projects, and Dissertations*. 944.
https://scholarworks.lib.csusb.edu/etd/944

SECURITY PRACTICES: KEEPING INDIVIDUALS SAFE AND AWARE IN THE CYBER WORLD

A Project
Presented to the
Faculty of
JHB College of Business and Public Administration,
California State University
San Bernardino

by
Annie Respicio
June 2019

Approved by:

Harold Dyck, PhD., Chair

Date

Conrad Shayo, PhD, Reader

Jay Varzandeh, PhD., Chair, Information & Decision Sciences Department

Dedication

To my beloved parents, words cannot even begin to express my appreciation for the both of you. Thank you for your endless support and unconditional love.

To my sister Alicia, brother-in-law Adriell, niece Izzy, and my overly adorable nephews Mateo and Mason. Thank you for your continued support and for the endless supply of giggles along the way.

Abstract

We currently live in a day and age where nearly everyone uses electronic devices and connects to the web. Whether it be from a desktop, laptop, or smartphone, staying connected and having information at your fingertips is easier than ever. Although technology has become so intermingled with our daily lives, the idea around security is not as momentous as it should be. As mentioned by the Multi-State Information Sharing and Analysis Center (MS-ISAC), “based on recent statistics, the average unprotected computer can be compromised in a matter of minutes. The majority of individuals who thought their computers were safe…were wrong.” (MS-ISAC 2)

This paper specifically investigates what types of security practices individuals in Southern California are aware of, how much of these practices are actively implemented and how can we not only further spread awareness, but also keep them engaged in these practices. This study shows that most of the participants feel confident about their level of knowledge regarding basic cyber security practices. Similarly, they were also confident in their active and frequent implementation of security practices.

Nonetheless, it is imperative that implementing security measures become an active part of people’s behavior. As technology and interconnectedness continues to grow, security will only become even more at risk. Since it is a difficult task to change the behavior of people, this study suggests the best route is to begin consistently teaching people at a young age. By doing so, many of these practices can become embedded within people and nearly function as second nature as they mature. Although this suggestion does not focus on security awareness and implementation on those individuals who currently use smartphones, computers, and other

devices, it is a sure way of ensuring the future populations become more engaged in understanding the importance of security measures and practice them.

Table of Contents

Introduction

Cyber security specialists can sit around all day conjuring up ways to keep their systems and networks more secure. They may discuss different tools they've used to monitor their network, like Wireshark. They may discuss access control lists to ensure only what they want to get through can get through. They may also even discuss reverse ssh between their computer, raspberry pi, and Google Cloud.

All of this can very well sound like a foreign language to people who do not understand technology. In turn, many people become intimidated and resort to the mentality of "I don't know anything about security" and leave that job up to the specialists. In reality, security is also the responsibility of the individual user; there are numerous "little" steps individuals can take to make their devices and networks more secure. No matter how big or small, enhancing device and network security from home makes it harder for the "bad guys" to get in.

With the idea that adhering to basic security steps at an individual level is extremely beneficial for everyone, it's interesting to explore what types of security practices individuals are currently aware of. Furthermore, it's also interesting to understand whether or not individuals actively implement these security practices they are aware of. Lastly, this study will include a possible solution to continuously educate and engage individuals with basic security practices.

The Problem Statement

There is an understanding that individuals need to partake in cyber security practices to reduce the risks of cyber threats. In the past, there have been many campaigns created in attempt to promote cyber security awareness, as well as many studies conducted to solve the issues regarding the subject at hand. Despite all this effort, there is still a lack of security awareness and engagement from individual users worldwide. This study first aims to understand the current level of security awareness and engagement of individuals in Southern California, primarily in Los Angeles County and the Inland Empire. Secondly, a suggestion will be proposed in the hopes of creating a society that is prepared to engage in protecting themselves against cyber threats.

Literature Review

There is a lot of research out there that revolves around the notion that merely educating individuals is not enough. For example, the paper "Why do they fail to change behavior?" states that "the primary purpose of cyber security-awareness campaigns is to influence the adoption of secure behavior online. However, effective influencing requires more than simply informing people about what they should and should not do: they need, first of all, to accept that the information is relevant, secondly, understand how they ought to respond, and thirdly, be willing to do this in the face of many other demands." (Bada, Sasse, and Nurse 2) These are critical factors to keep in mind while this study itself attempts to propose a solution towards a more secure society.

Additionally, a theoretical model has also been created that focuses on enforcement. The main idea around this is that individuals need to be forced in some way to implement security measures before proceeding. For example, an individual user would need to adhere to particular security measures before being able to access a website, even a well-known site, because it may contain malware. This is referred to as the E-Awareness Model, or E-AM. (Kritzinger and von Solms) Although this may sound like a decent idea and is a possible solution, there are a lot of issues that come along with attempting to achieve it. Those include:

- Social impact- user acceptance of the model

- Legal impact- assumes partial responsibility on ISPs (internet service providers) and if individuals can hold ISPs responsible
- Lack of technical details- this model is purely theoretical and no technical planning has been shared

Because of the issues mentioned above and lack of specifications of the E-AM model, this idea may not seem feasible, at least not at present time. It is also critical to take this model into consideration when proposing a solution here.

Another study from Malaysia focused on internet and device usage of children in public schools. In their findings, they included some interesting results. For example, nearly 50% of 7 to 9 year olds who were surveyed have social media accounts. Also, 92.47% of students 13-17 years of age have social media accounts. (Zahri, 2017) Through the alarming statistics provided, it is evident that now nearly all age groups are accessing the web. Since these survey questions were aimed at understanding the behavior of young students, the questions presented in this study's survey need to be a unique set as the target participants are different.

Other researchers have also attempted to propose solutions to promote cyber security awareness and engagement. An interesting approach is a video game that was developed for cyber security training and awareness. CyberCIEGE "is described as a security awareness tool that can support organizational security training objectives while engaging typical users in an engaging security adventure." (Cone, 2007) It is said to be utilized by a variety of organizations and can be effective for general computer users. An implementation of a video game to promote cyber security awareness is an approach that would be more engaging and hands-on for users. Although, like any video game, gaining and maintaining users on the system would be a challenge. A video game of the like can be a part of the solution, but it is not the whole answer to the issue at hand.

It is apparent that many studies have been conducted around the area of cyber security awareness. Despite all this effort, we have yet to come to any real solution and implementation in order to promote awareness and engagement, hence the reason why this study is being pursued. This study focuses on Southern California, primarily Los Angeles County and the Inland Empire, because these areas are heavily populated and include a diverse population. With these characteristics, somewhat unique approaches may be required as opposed to areas with less population or diversity.

Literature Review

Annie: I think the Literature Review Section should be placed here. i.e, a number of studies have been done on the problem. So and so did this and found this… but highlighted the need to conduct further studies on this… etc. and finally stating why you are pursuing this area.

The Methodology

In order to attempt to answer the problem question, the approach is dissected into two parts. First, we need to understand what types of security practices individuals in Southern California (primarily Los Angeles County and the Inland Empire) know and what security practices they actively implement. This will be achieved by collecting data via a survey. Thereafter, we can analyze the data and propose a possible solution to the problem question.

The questions used in this survey were curated by the researcher, who created questions of her own. Comparable studies have asked similar questions, such as: 1) Are your passwords over 8 characters long? 2) Do you respond to emails/messages without knowing the source? And 3) Do you keep your software up to date and use an anti-virus scanner? Although similar questions have been used in various other studies, it was important to have a unique set of questions for the Los Angeles County and Inland Empire demographic. The main reason for this is because these areas are highly diverse. For some, English may not be their first language, so it is imperative to have a set of questions that are simple enough to be inclusive yet obtain accurate responses. In addition, the survey should be simple and short to ensure participants complete the survey.

The IRB Process, Data Collection and Analysis

Survey key details

The research method chosen to help understand the current knowledge and practices of individuals in Southern California regarding security practices is to send out a survey asking various questions. There were many steps involved to design and get approval to send out the survey. The steps regarding the IRB training, IRB application, and full results of the survey can be reviewed in the appendix.

As detailed in the IRB application, here are a few key notes to know regarding the survey:

- Survey was sent to CSUSB colleagues as well as people within the researcher’s personal network
- Survey participants were asked to share the survey with their personal network as well
- Survey participants had to be at least 18 years of age

- The target audience would not be involved within the technology industry, although a few participants are acceptable (provide the number of few—i.e. maximum of ## or limited to ##)

The questions given in this survey were designed around top security tips given by two University of California colleges, UC Berkeley (UC Berkeley) and UC Santa Cruz. (UCSC, 2016). A few of the security tips included are:

- Keep your software up to date
- Practice good password management
- Never leave devices unattended
- Don’t install or download unknown or unsolicited programs/apps

Graphics to visualize and understand the data

Once the survey was closed, we analyzed the data we had collected to gain an understanding of what individuals currently know and what they actively practice. This study had a total of 49 participants who are in different age ranges and occupations. (Please consider using only the graphics here. Leave the actual data in the Appendix.). This way your narrative will look cleaner. Present the analysis on each graphic as it is presented. Here is an example:

Figure 2.2 provides a histogram of the ages of the respondents. About 63% of the respondents’ age was between 18 and 35 years old. Only 10% were between 36 and 45 years old, and the remaining 27% were above 46 years old and above.

Question 8: Age

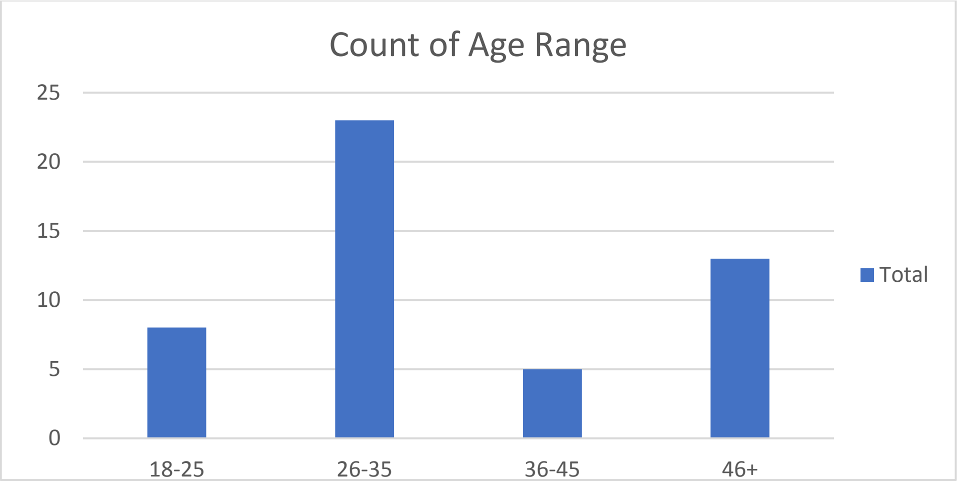


Figure 1.1 Count of Age Histogram

Figure 1.1 provides a histogram of the ages of the participants. About 63% of the participants age was between 18 and 35 years old. Only 10% were between 35 and 45 years old, and the remaining 27% were 46 years old and above.

Question 1: My passwords have a combination of all these: upper case letters, lower case letters, numbers and special characters.

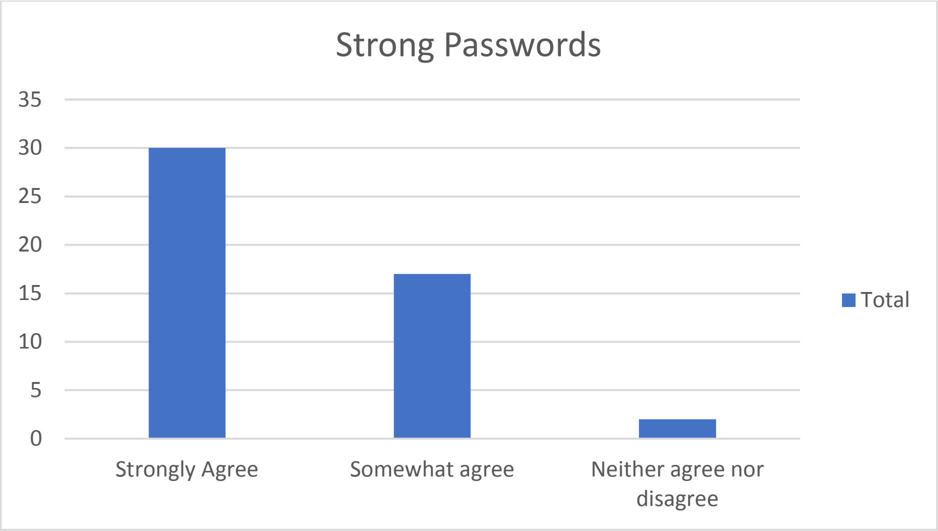


Figure 1.2 Q1 Histogram

Figure 1.2 provides a histogram of the responses for question 1 regarding password strength. About 61% of the participants strongly agree that their passwords include upper case letters, lower case letters, numbers and special characters. About 35% of the participants somewhat agree, while only 4% neither agree nor disagree. None of the participants reported that they either somewhat disagree or strongly disagree.

Question 6: I am familiar with basic security practices I should be following.

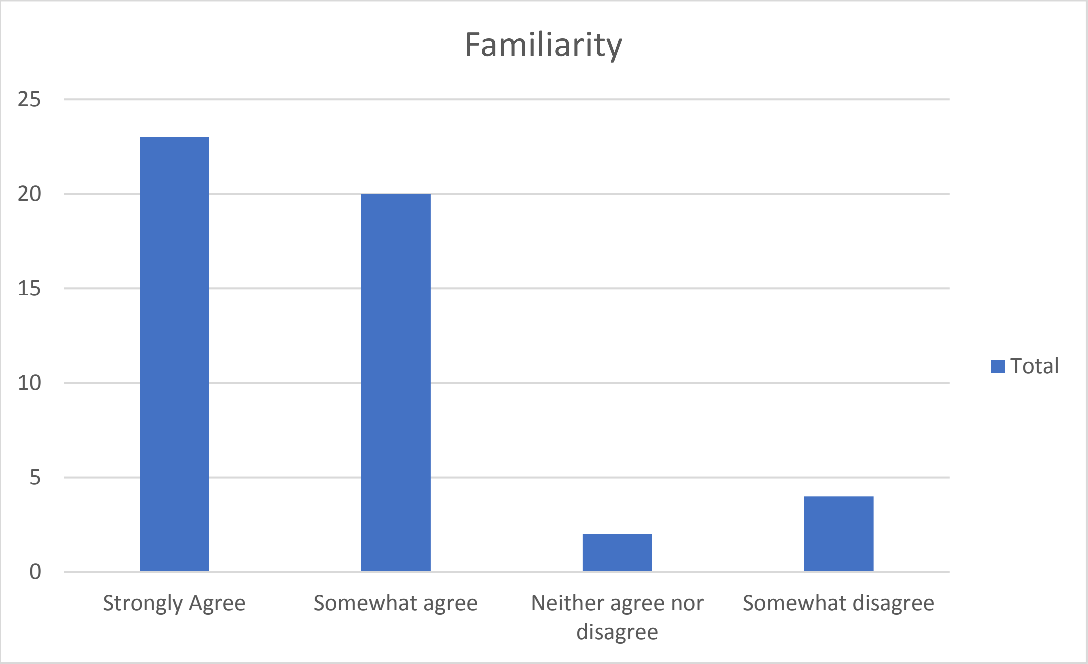


Figure 1.3 Q6 Histogram

Figure 1.3 provides a histogram of the responses for question 6 regarding familiarity of basic cyber security practices. An overwhelming amount of the participants, approximately 88%, reported to either strongly agree or somewhat agree. 4% neither agree nor disagree, while 8% somewhat disagree.

Question 7: I actively and frequently follow the basic security practices suggested for everyone.

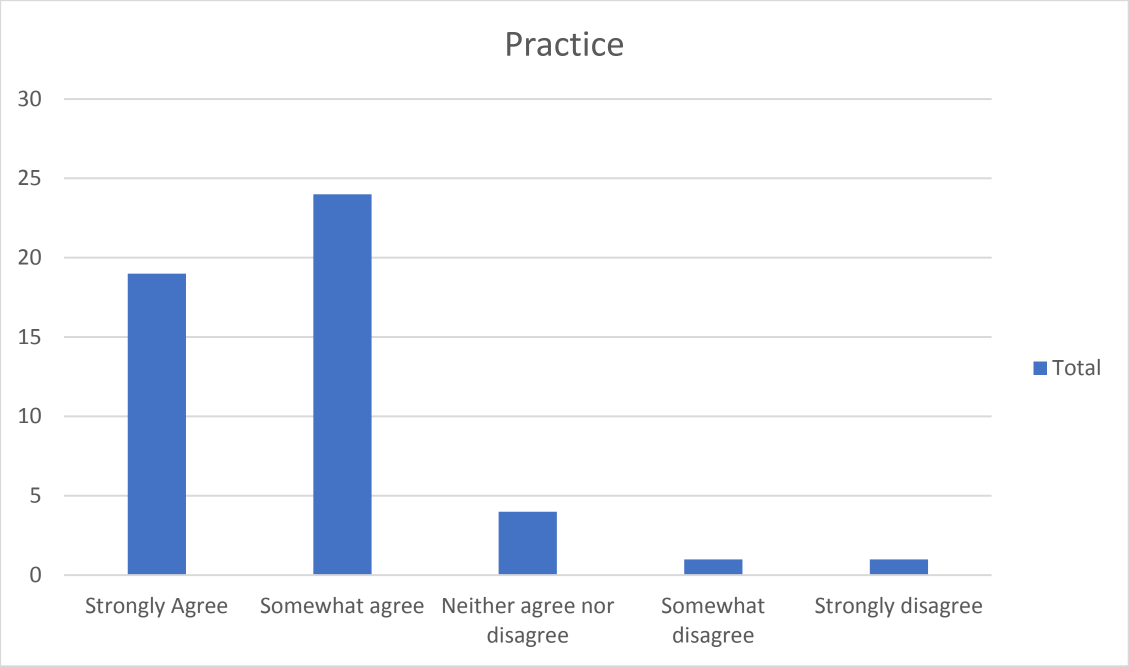


Figure 1.4 Q7 Histogram

Figure 1.4 provides a histogram of the responses for question 6 regarding engagement of basic cyber security practices. 88% reported to either strongly agree or somewhat agree that they actively and frequently follow basic practices. 8% neither agree nor disagree, while 4% either somewhat or strongly disagree.

Age vs. Familiarity

Count of Q8	**Column Labels**				
Row Labels	**18-25**	**26-35**	**36-45**	**46+**	**Grand Total**
Strongly Agree	2	11	3	7	23
Somewhat agree	3	11	2	4	20

Neither agree nor disagree		1		1	2
Somewhat disagree	3			1	4
Grand Total	**8**	**23**	**5**	**13**	**49**

Figure 2.1 Age and Familiarity Cross Tabulation Count

Age vs. Practice

Count of Q8	**Column Labels**				
Row Labels	**18-25**	**26-35**	**36-45**	**46+**	**Grand Total**
Strongly Agree	1	8	3	7	19
Somewhat agree	6	12	2	4	24
Neither agree nor disagree		3		1	4
Somewhat disagree				1	1
Strongly disagree	1				1
Grand Total	**8**	**23**	**5**	**13**	**49**

Figure 2.2 Age and Practice Cross Tabulation Count

Data Analysis

From the data shown for Question 6 in Figure 1.3, it seems like most people believe they are familiar with basic security practices. 47% of the participants reported that they strongly agree that they are familiar with them, while 41% reported that they at least somewhat agree. Only 12% of the participants believe that they do not agree, do not disagree, or somewhat disagree. That being said, 88% of the participants feel confident that they are familiar with basic security practices.

Let’s see how the participants’ familiarity with basic security rules compare with what they actively and frequently practice, shown in Figures 1.4. 39% of the participants strongly agree and 49% somewhat agree. 8% neither agree nor disagree, 2% somewhat disagree, and 2% strongly disagree. With that data collected, 88% of the participants fall into the confident level of strongly agree or somewhat agree. Although this is the same percentage as familiarity, there was a 7% drop from the strongly agree category to the somewhat agree. That is an acknowledgement that awareness does not equal action.

There seems to be a popular pre-conception that the younger generations are better with technology and therefore should know more about security rules and practices. Alternatively, the older generation is seen to be less technically advanced, therefore contain less knowledge regarding security. Let’s see how those hypotheses stand up against the data we’ve collected here.

In order to do so, a cross tabulation between age (question 8) and the responses regarding familiarity (question 6) had to be created. This helps us see what age groups reported which responses and is shown in Figure 2.1. There is an interesting find here in the data. If you take a look at the responses for “somewhat disagree,” you will see that there are 4 total responses. Three of those responses came from the 18-25 years old age group while the one other response came from the 46+ years old age group. It is interesting that the age group with the highest number of “somewhat disagree” responses came from the youngest age group.

We also did a cross tabulation between age (question 8) and the responses regarding practice (question 7) as shown in Figure 2.2. There is 1 response that answered “strongly disagree" to frequently and actively practicing security measures and that came from the age group of 18-25 years. Similarly, there is 1 response for "somewhat disagree" and that came from the 46+ years of age. Most of the participants in the age group responded with positive/confident responses of "somewhat agree" or "strongly agree."

Solution for Awareness and Engagement

Middle Ground Solution

After reviewing the existing studies and literature, it seems that a solution that shares a middle ground between these opposing views would be most successful. Merely educating individuals has proven to be insufficient. The idea of enforcing users to implement security features before being able to proceed is purely theoretical—and we can highly assume that this would be very difficult for the public to accept based off social and psychological studies. So, what is the middle ground?

This middle ground solution should be:

- Feasible
- Easy for individuals to digest
- Easy for individuals to understand the action items necessary
- Non-threatening approach; should be fun and engaging

Example of a Middle Ground Solution Implementation

At this point of our current state, it would be extremely beneficial if we start by targeting individuals at a young age. By doing so, we can instill these security practices as habits within their daily lives. "The development of skills associated with effective decision-making are acquired over time.” (Berson) For the duration of their education, we can educate them as to why these security practices are important. Instead of merely stating “do this,” we can also say “these are the risks you take by not doing so.” Hearing these enough will be a lot more impactful than being a full-grown adult and going through one day of security training at work. Many are in agreement that students need education that prepare them to function and participate in this technology-driven society. (National Council for the Social Studies, 2006)

Many may ask “well what about the older generations who already use devices and need security?” This population would need a different solution other than what is being proposed. The proposed suggestion is looking into the bigger picture of creating a society where practicing security is nearly second nature. Finding a solution for the current device users is out of scope for this particular research.

Now that we understand the target population for this solution, how would we go about doing that? The first, and arguably most obvious, is to start introducing security practices at schools. We are not suggesting a full course dedicated to cyber security or anything—that would likely be impractical. However, even 5-10 minutes a day sharing a security rule, the importance of it, and the risks that are involved by not doing so would be greatly impactful. Students can even take out their phone for those few minutes and follow along. For example, if the instructor is reviewing how to set up two-factor authentication on a mobile device, students can follow along and attempt to implement it on their own mobile device.

It is very common that high school students purchase a laptop soon after graduation (if they do not already have one, of course) because they will be attending college soon. However, I’m sure many of those students have never even heard of a firewall. If we were to implement this solution, they would have had around 12-13 years of exposure to security practices and will likely retain some of them.

The majority of us can agree security is extremely important, but the talks and thoughts about what we as individuals can do does not happen nearly enough. Although some campaigns have attempted to educate people, getting them to change their behavior has proven to be extremely difficult. Therefore, we must start where we know for certain we can—and that is children. Children absorb information quickly and this is also the time in which habits are formed.

Although this may seem like a nuisance to put this responsibility on schools and teachers, it is the surest way that the children will be able to learn. We teach children about nutrition and sex because of the impact it has on their daily and overall life. This is absolutely the same case for security and it should begin to be held up to the same importance.

A similar but alternative approach is to create a standardize lesson for that particular demographic that can easily be presented in class. For example, a series of YouTube videos can be created and would each last for only a few minutes long. These videos would be presented in class and a short discussion can happen thereafter. This suggestion would standardize the security practices being taught as well as alleviate much of the responsibility from teachers.

Potential Hurdles

Any major change or shift would have challenges that lie ahead of them. It is important to understand what those challenges are and determine ways to navigate through them. We won't specifically figure out solutions to each of the potential issues, but here are some of the biggest challenges the solution provided in this paper can have.

- Added pressure on teachers/instructors

- Training for the teachers/instructors to have properly knowledge and skills to teach the students

Conclusion

After conducting the survey, it is clear that participants feel confident about their knowledge and practice in regard to basic security rules. What was a surprising find is that there were more individuals within the 18-25 age group who felt just as unconfident as those who are 46+ years. This is interesting because it defies that preconception of the youth knowing more about security than those who are in older generations. Nonetheless, the confidence level of the participants is higher than originally anticipated.

Although changing the behaviors of the current population is ideal, it would be extremely difficult to do. Therefore, a more conceivable and plausible solution would be to begin teaching students about security at a young age. This teaching would include explaining what the threat is, what the risks are, as well as what those individuals would need to do to protect themselves against threats. Consequently, individuals who know how to maintain secured networks will also take this knowledge and practice with them after school. This is beneficial to the workforce—employees will enter with knowledge and practice on maintaining a secured network. Should students choose to pursue their education, colleges will also be at less risk if students enter already engaged in security practices. Although the information provided concludes this study, there is intent to pursue designing and implementing a standardized lesson for children in school.

References

Bada, Maria, Angela M. Sasse, and Jason RC Nurse. "Cyber security awareness campaigns: Why do they fail to change behaviour?." *arXiv preprint arXiv:1901.02672* (2019).

Berson, Ilene R., Michael J. Berson, Shreya Desai, Donald Falls and John Fenaughty. "An Analysis of Electronic Media to Prepare Children for Safe and Ethical Practices in Digital Environments." 2007. https://www.citejournal.org/volume-8/issue-3-08/social-studies/an-analysis-of-electronic-media-to-prepare-children-for-safe-and-ethical-practices-in-digital-environments/

Cone, Benjamin D., et al. "A video game for cyber security training and awareness." *Computers & security* 26.1 (2007): 63-72.

Kritzinger, Elmarie, and Sebastiaan H. von Solms. "Cyber security for home users: A new way of protection through awareness enforcement." *Computers & Security* 29.8 (2010): 840-847.

National Council for the Social Studies. "Technology position statement and guidelines." 2006. http://www.socialstudies.org/positions/technology

The Multi-State Information Sharing and Analysis Center. "Cyber Security Awareness Handbook." MS-ISAC, 2005. http://www.cscic.state.ny.us/msisac/index.html

UCSC. "`Top 10 List" of Good Computing Practices.'" UCSC, Mar. 2016, its.ucsc.edu/security/top10.html.

UC Berkeley. "`Top 10" Secure Computing Tips.'" UC Berkeley, https://security.berkeley.edu/resources/best- practices-how-to-articles/top-10-secure-computing-tips.

Zahri, Yunos, Ab Hamid R. Susanty, and Ahmad Mistaffa. “Cyber Security Situational Awareness among Students: A Case Study in Malaysia. Vol: 11, No: 7, 2017.

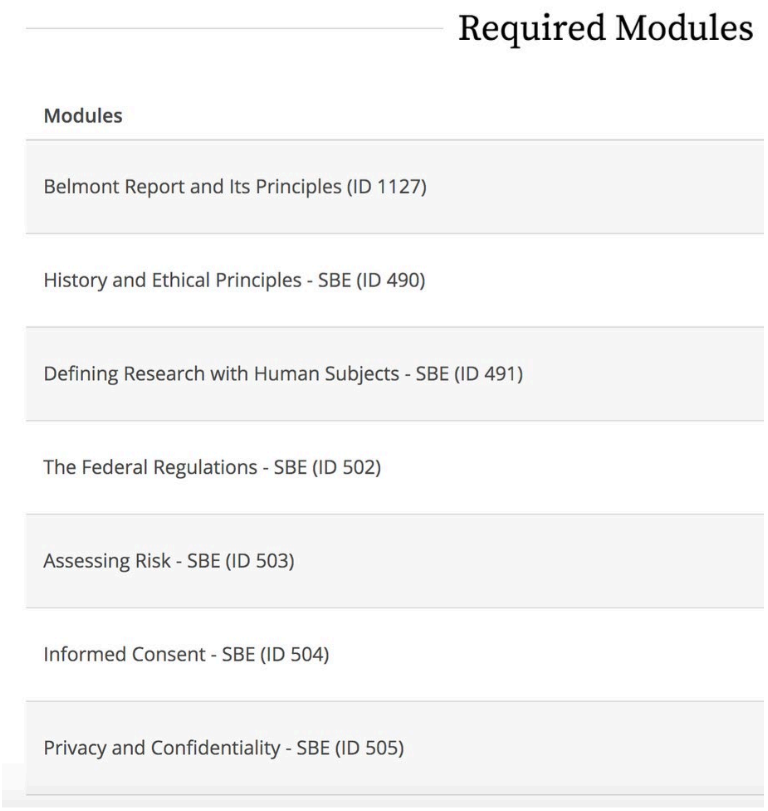
Appendix

IRB

For those who are looking to conduct any study that requires humans as subjects in the research, it is very likely you will require approval from the IRB. The purpose of an IRB, which stands for Institutional Review Board, is to ensure that any study involving human subjects are conducted ethically and pose minimal risk its participants. The board reviews each study in detail and ensures the study seems ethically sound. If the Institutional Review Board approves the application, the study can then proceed. The IRB process may require some time to complete, so it is important to keep in mind when designing your study if time is a factor.

Complete the IRB Training

The CSUSB IRB website contains a url needed to complete the IRB training. Completing this training is the very first step that needs to be done in order to proceed. Both my advisor, Dr. Harold Dyck, and myself had to complete this training. The training consists of eight different modules. Each of these modules explore different situations that may arise when conducting studies with human subjects. For example, you learn different rules to follow if prisoners or pregnant women will be participants in your study. After each module, there is a quiz that must be completed. Once each module and quiz has been successfully completed, you are given an IRB completion report.



Required Modules

Modules
Belmont Report and Its Principles (ID 1127)
History and Ethical Principles - SBE (ID 490)
Defining Research with Human Subjects - SBE (ID 491)
The Federal Regulations - SBE (ID 502)
Assessing Risk - SBE (ID 503)
Informed Consent - SBE (ID 504)
Privacy and Confidentiality - SBE (ID 505)

Figure 1.1 IRB Training Example

IRB Application

The CSUSB IRB website also provides a link to the portal in order to submit your IRB application. The main purpose of this application is so the IRB board can review the proposed study and all of its details to determine whether or not it is ethnical and poses minimal risks to the human participants. Depending on the study's intended participants, the IRB review can take anywhere from one week to one month to be approved or disapproved. It is also important to note that the researcher absolutely cannot begin their research, in this case send out the survey, until the IRB application has been approved.

It is during this process that all of the details and design of the study is included. This included the target/intended audience, what tools will be used, how the data collected will be stored and secured, etc. Therefore, it was imperative to completely design out the survey at this point.

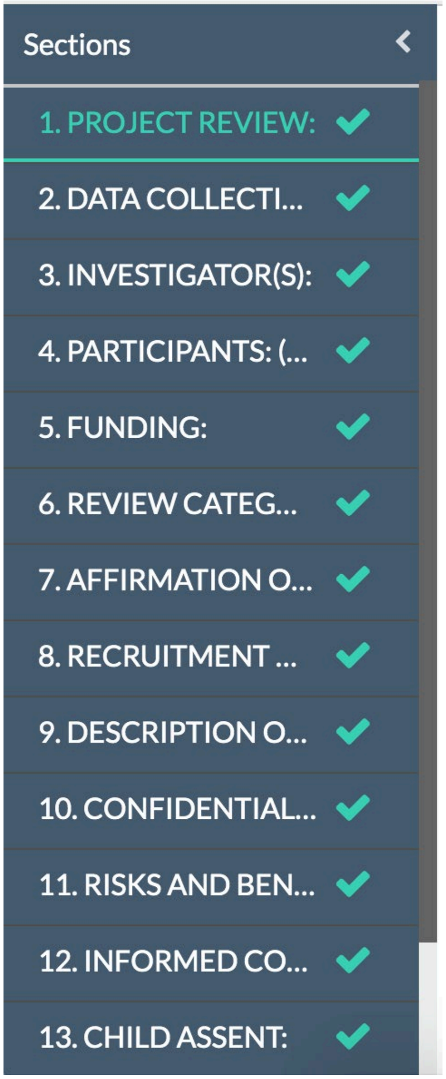


Figure 1.2 IRB Application

Survey questions and Qualtrics

Qualtrics is the chosen program to send out the survey for this study. The first reason is because it was easily accessible to the researcher, as CSUSB provides access to it for all its students. Second, Qualtrics is a powerful tool that would provide the researcher with customization and flexibility with the survey.

Once logged in, the survey was created according to the details submitted within the IRB application. First, the ten questions were entered. These questions were designed primarily based off of security tips provided on the UC Santa Cruz and UC Berkeley websites. The questions included in the survey are as follows:

1. My passwords have a combination of all these: upper case letters, lower case letters, numbers and special characters.

2. I use two-factor authentication on my devices.

3. I always keep my software up to date.

4. I open links or attachments sent to me via email, even if the sender is unfamiliar to me.

5. I frequently visit unfamiliar/unverified websites.

6. I am familiar with basic security practices I should be following.

7. I actively and frequently follow the basic security practices suggested for everyone.

8. Age

9. Occupation

10.City

Then, the set of questions were set as a multiple-choice type. By doing so, participants are able to select one answer out of five options that closest related to them. For questions 1-7, the answer options were as follows:

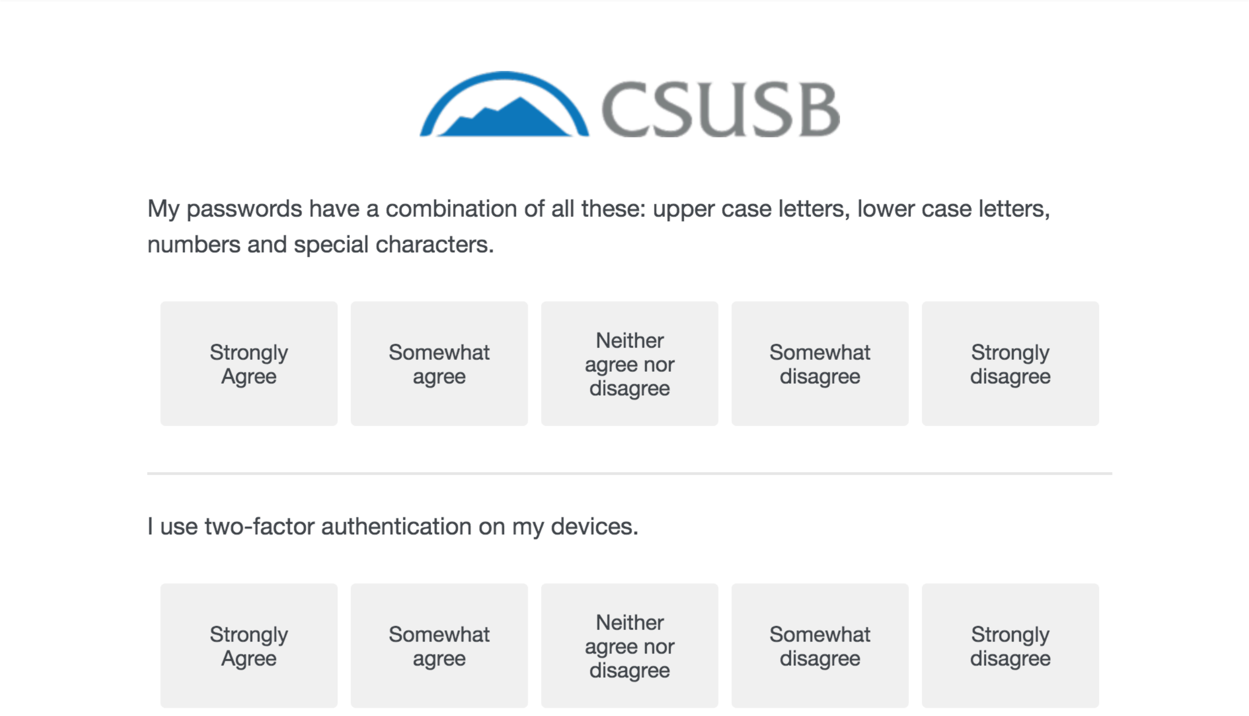
- Strongly agree
- Somewhat agree
- Neither agree nor disagree

- Somewhat disagree
- Strongly disagree

For question 8 regarding age, the four options presented to participants are as follows:

- 18-25 years
- 26-35 years
- 36-45 years
- 46+

For question 9 regarding occupation and question 10 regarding city, each has a text box for users to manually enter their response.



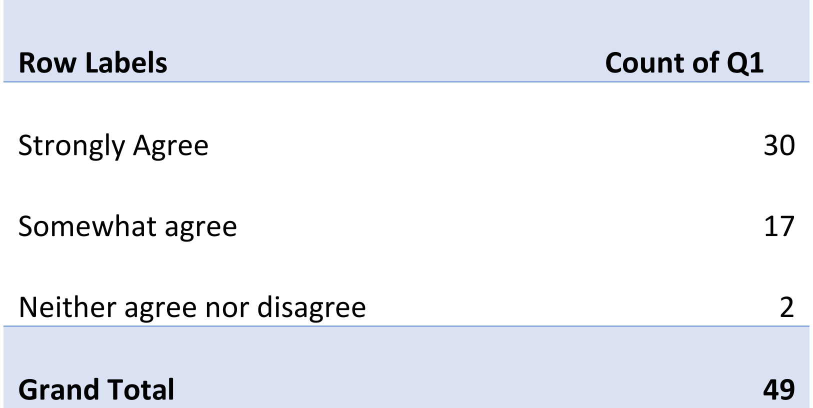
My passwords have a combination of all these: upper case letters, lower case letters, numbers and special characters.

I use two-factor authentication on my devices.

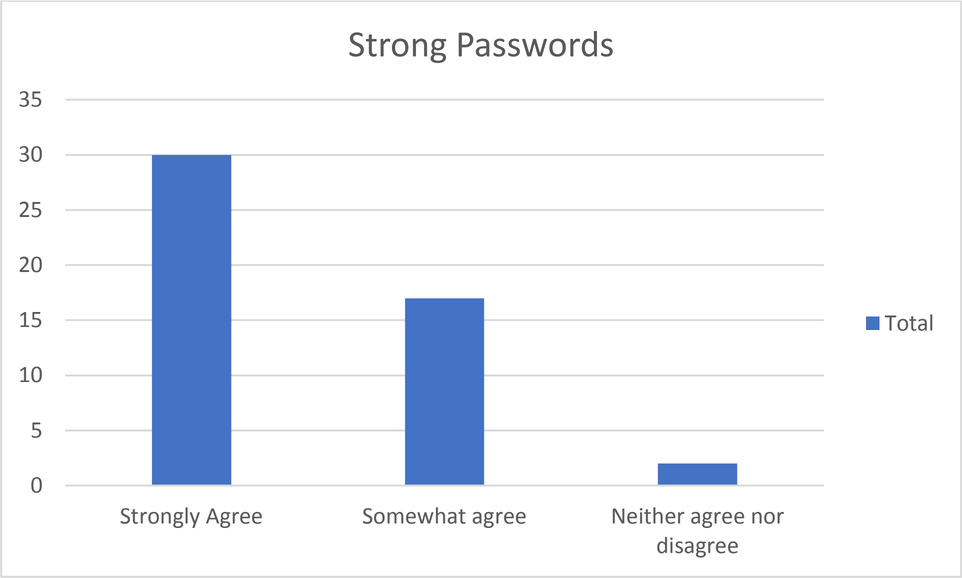
Survey Results

This section will provide a complete view of the results from the survey. The survey question, a pivot table and histogram will be displayed for questions 1-8.

Question 1: My passwords have a combination of all these: upper case letters, lower case letters, numbers and special characters.

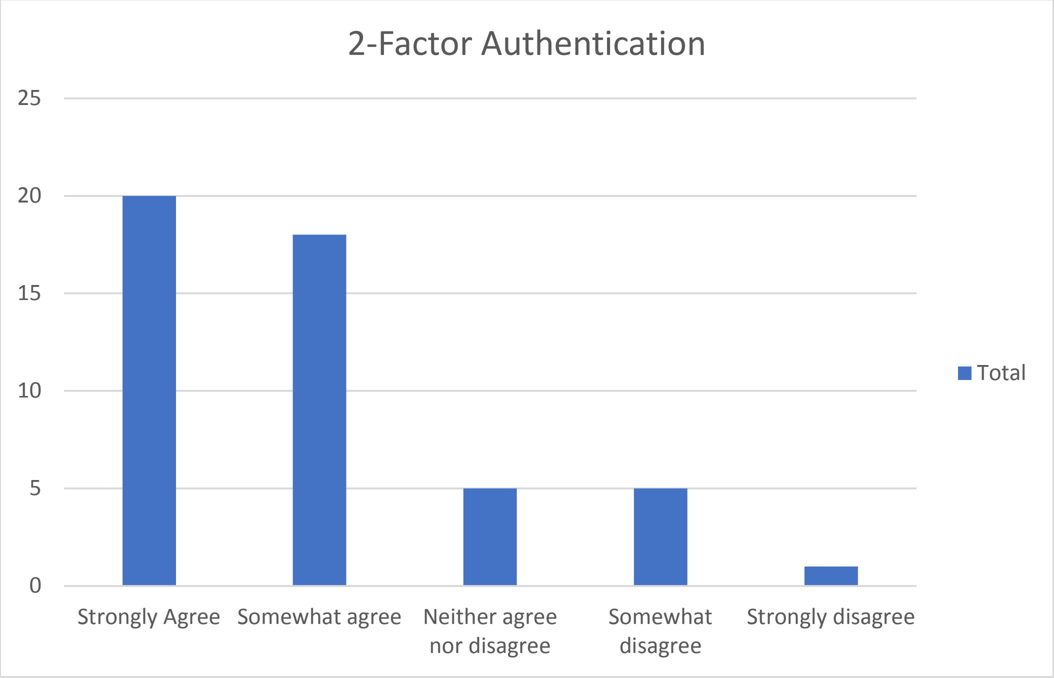


Row Labels	Count of Q1
Strongly Agree	30
Somewhat agree	17
Neither agree nor disagree	2
Grand Total	**49**



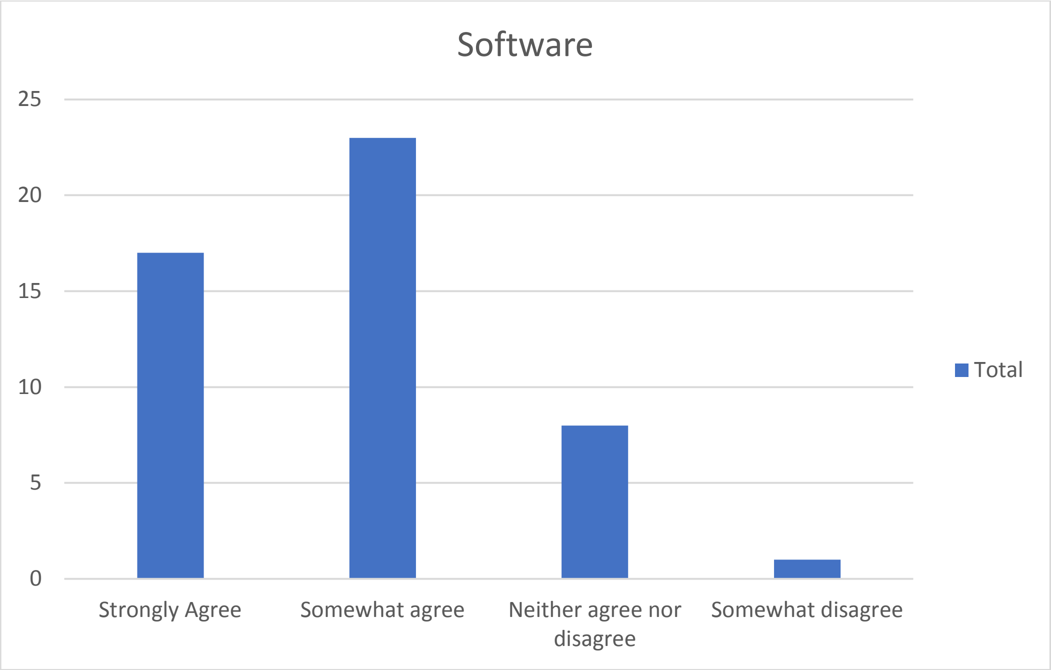
Question 2: I use two-factor authentication on my devices.

Row Labels	Count of Q2
Strongly Agree	20
Somewhat agree	18
Neither agree nor disagree	5
Somewhat disagree	5
Strongly disagree	1
Grand Total	**49**



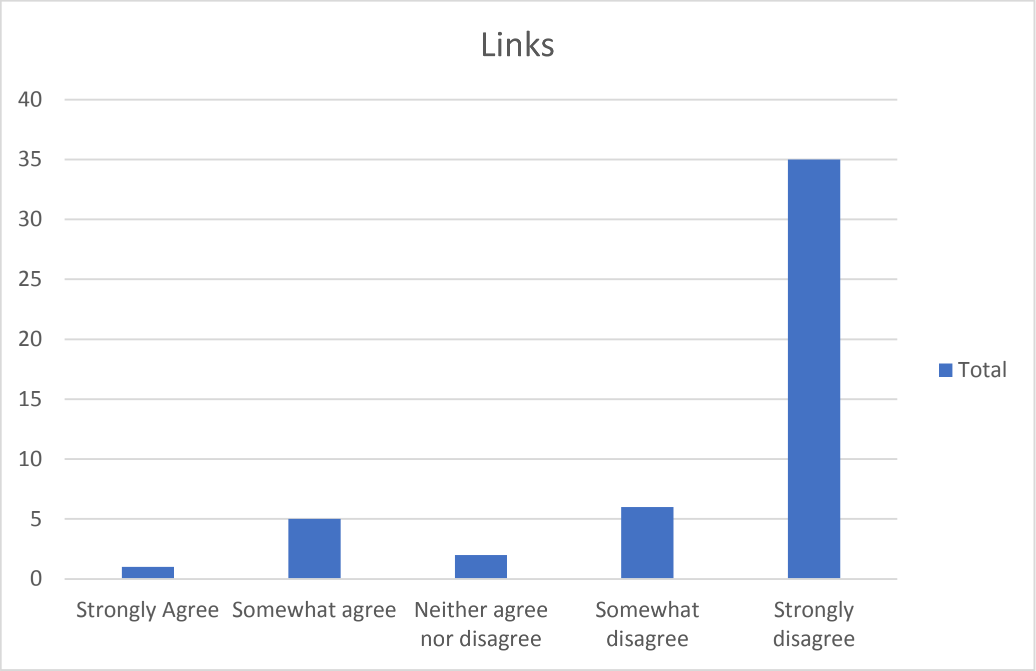
Question 3: I always keep my software up to date.

Row Labels	**Count of Q3**
Strongly Agree	17
Somewhat agree	23
Neither agree nor disagree	8
Somewhat disagree	1
Grand Total	**49**



Question 4: I open links or attachments sent to me via email, even if the sender is unfamiliar to me.

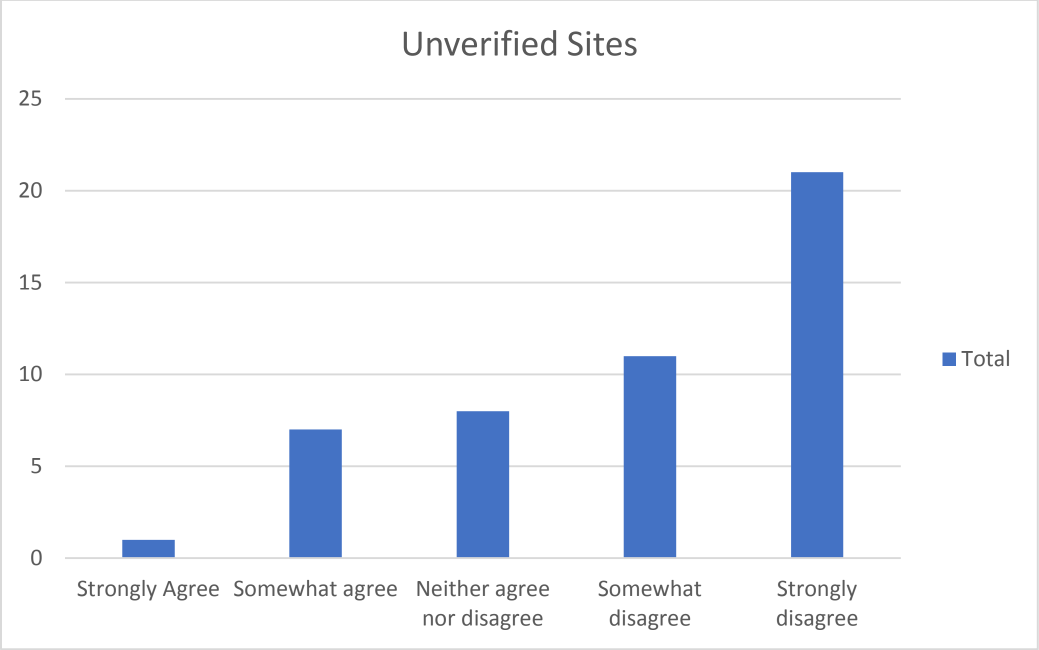
Row Labels	**Count of Q4**
Strongly Agree	1
Somewhat agree	5
Neither agree nor disagree	2
Somewhat disagree	6
Strongly disagree	35
Grand Total	**49**



Question 5: I frequently visit unfamiliar/unverified websites.

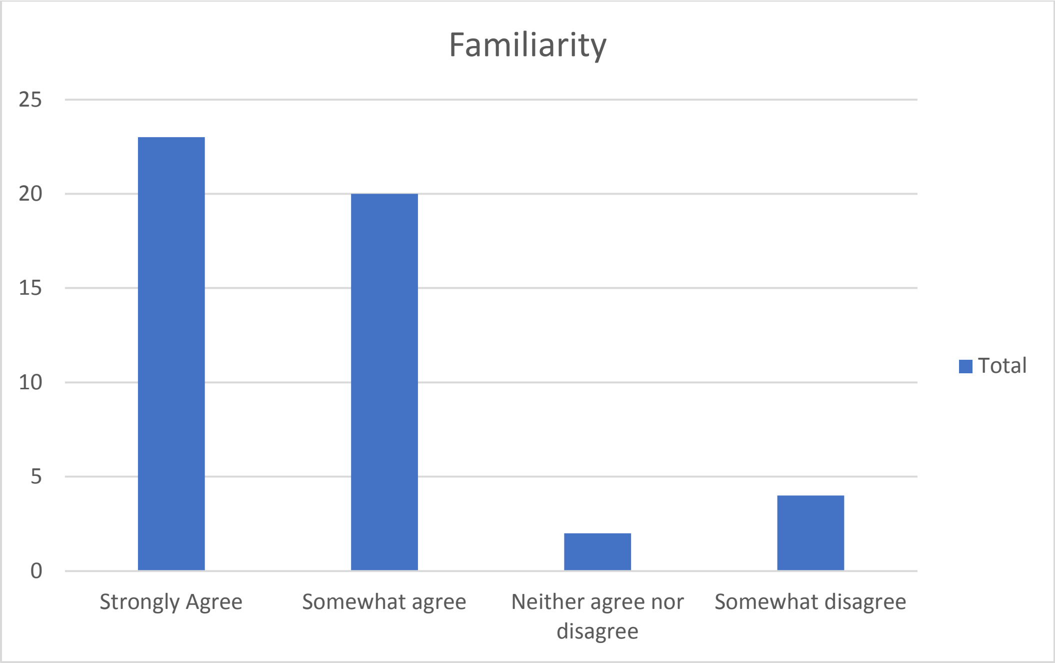
*Note that one participant skipped answering this question, resulting in a total count of 48 participants.

Row Labels	Count of Q5
Strongly Agree	1
Somewhat agree	7
Neither agree nor disagree	8
Somewhat disagree	11
Strongly disagree	21
Grand Total	**48**



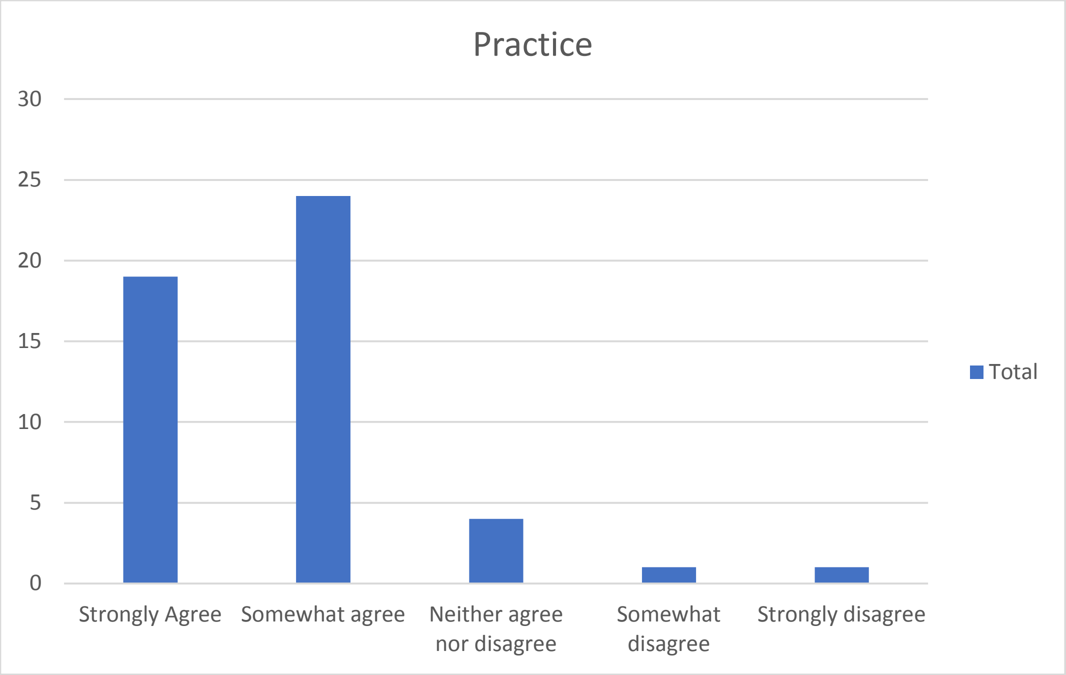
Question 6: I am familiar with basic security practices I should be following.

Row Labels	**Count of Q6**
Strongly Agree	23
Somewhat agree	20
Neither agree nor disagree	2
Somewhat disagree	4
Grand Total	**49**



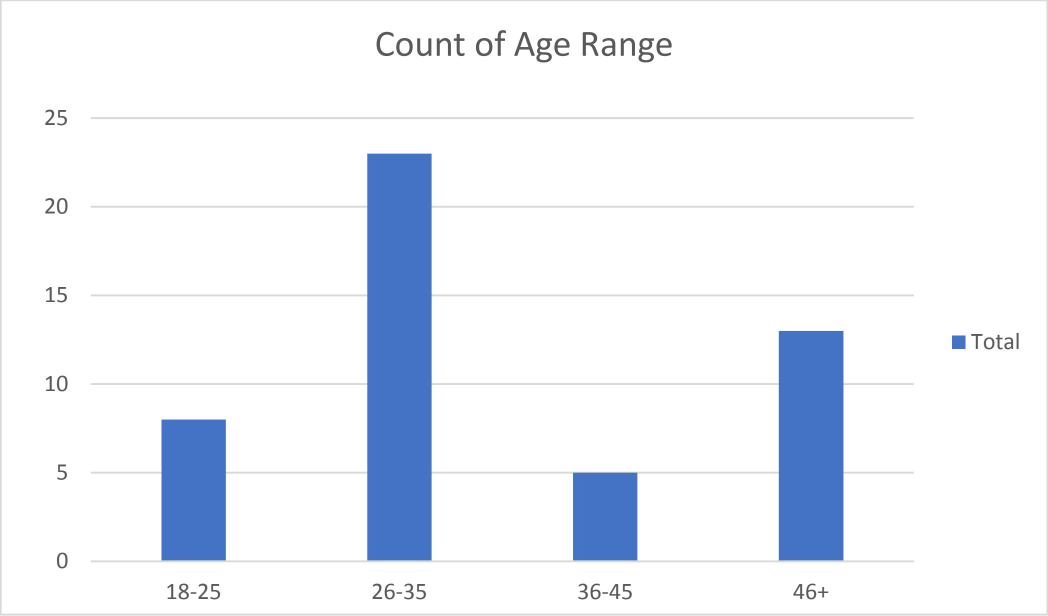
Question 7: I actively and frequently follow the basic security practices suggested for everyone.

Row Labels	**Count of Q7**
Strongly Agree	19
Somewhat agree	24
Neither agree nor disagree	4
Somewhat disagree	1
Strongly disagree	1
Grand Total	**49**



Question 8: Age

Row Labels	**Count of Age Range**
18-25	8
26-35	23
36-45	5
46+	13
Grand Total	**49**



Question 9: Occupation

The participants greatly varied in their occupations. Some examples include students, members of the military, recruiting coordinators, retail employees, sous chefs, servers, and music producers.

Question 10: City

The participants were located in Southern California, primarily in Los Angeles County and the Inland Empire. Some examples of cities within Los Angeles County are Culver City, El Monte, Los Angeles, Pasadena, and Reseda. Some examples cities in the Inland Empire are Riverside, Moreno Valley, San Bernardino and Ontario.