2023 Annual Conference & Exposition
Baltimore Convention Center, MD | June 25 - 28, 2023
The Harbor of Engineering Education for 130 Years
ASEE
Paper ID #39751

Examining the Impact of Early Cybersecurity Education in the Selection of Cybersecurity as a Career among High School Senior and University Freshmen Students

Sai Sushmitha Sudha
SaiSuma Sudha
Dr. Ahmad Y. Javaid, The University of Toledo

Ahmad Y. Javaid received his B.Tech. (Hons.) Degree in Computer Engineering from Aligarh Muslim University, India in 2008. He received his Ph.D. degree from The University of Toledo in 2015 along with the prestigious University Fellowship Award. Previously, he worked for two years as a Scientist Fellow in the Ministry of Science & Technology, Government of India. He joined the EECS Department as an Assistant Professor in Fall 2015 and is the founding director of the Paul A. Hotmer Cybersecurity and Teaming Research (CSTAR) lab. Currently, he is an Associate Professor in the same department. His research expertise is in the area of cyber security of drone networks, smartphones, wireless sensor networks, and other systems. He is also conducting extensive research on human-machine teams and applications of AI and machine learning to attack detection and mitigation. During his time at UT, he has participated in several collaborative research proposals that have led to a cumulative sum of ˜$12M (including all partners along with UToledo) in the funding of which $2.1M has been allocated specifically to him. Out of this ˜$12m, ˜$5.45M has been allocated to the University of Toledo. These projects have been funded by various agencies including the NSF (National Science Foundation), AFRL (Air Force Research Lab), NASA-JPL, Department of Energy, and the State of Ohio. He also played a critical role in the cultivation of a private gift to support the CSTAR lab for cyber security research. He has published more than 90 peer-reviewed journal, conference, and poster papers. He has also served as a reviewer for several high impact journals and as a member of the technical program committee for several reputed conferences.

Xiaoli Yang

Examining the impact of early cybersecurity education in the selection of cybersecurity as a career among high school senior and university freshmen students

Sai Sushmitha Sudha[1], Sai Suma Sudha[1], Ahmad Y Javaid[1], Quamar Niyaz[2], and Xiaoli Yang[3]
[1] The University of Toledo, Toledo, OH 43607, USA
{saisushmitha.sudha, saisuma.sudha, ahmad.javaid}@utoledo.edu
[2] Purdue University Northwest, Hammond IN 46323, USA
qniyaz@pnw.edu
[3] CS Department, Fairfield University, Fairfield, CT, United States.
xyang@fairfield.edu

Introduction

Cybersecurity is a fast-expanding field that is essential for shielding people, businesses, and governments from online dangers. There is no denying that the Internet and other digital media have altered how individuals collect, study, and create information/knowledge [1][2]. The action, process, capability, or state of information and communications systems and the data they contain being guarded against or defended against harm, unauthorized access use or alteration, or exploitation is another definition of cybersecurity [1]. When spending a lot of time online, all users, regardless of age, are subject to various cybersecurity threats [2]. Young individuals are a specific target for these cybercrimes due to their lack of expertise in cybersecurity and cyber-safe habits. Hackers are predicted to launch increasingly complex attacks on everything from autonomous vehicles to air traffic control systems, power grids, and nuclear plants in the upcoming years [3].

The need for knowledgeable cybersecurity professionals is expanding along with the usage of technology in our daily lives. Although there is a rising demand for cybersecurity education, many students are not exposed to it until they are at the undergraduate level or even later in their careers. Targeting high school students and university freshmen students, it is critical to promote cybersecurity education early to solve this issue. Every parent needs to have awareness about and skills in cyber parenting [9]. The need for innovation in providing cybersecurity education to local high school kids who do not have access to these burgeoning professions is pressing for minority-serving rural hybrid community institutions [10]. Along with companies and well-known individuals, many middle and high school pupils have become victims of cybercrime [4]. Students will gain the knowledge and skills they need to make wise decisions about their future employment as well as a greater awareness of the subject and its prospective career prospects.

Providing early cybersecurity education for high school students can help them develop the knowledge and skills they need to protect themselves and others from cyber threats. This can include learning about common types of cyber-attacks, such as phishing, malware, and social engineering. They can also learn about the best practices for maintaining security on their personal devices, such as using strong passwords, keeping software up to date, and being cautious when sharing personal information online. Additionally, as kids from underrepresented groups might not have the same access to information and resources concerning cybersecurity professions, early exposure to cybersecurity education can help boost the field's diversity and inclusivity. Furthermore, since it can help to develop a new generation of knowledgeable experts to fulfill the expectations of the industry, early cybersecurity education can also contribute to

addressing the present cybersecurity professional shortage and to be able to protect their digital assets, personal devices, and personal information.

In addition to protecting themselves, high school students who have cybersecurity education can also play a crucial role in protecting their families, friends, and communities from cyber threats. They can educate others about safe online practices and help to create a more secure digital environment for everyone. Despite the State of Ohio's sponsored initiatives that benefit students, including $89 million for top-notch summer and after-school activities, there has not been a lot of focus on cybersecurity education at the high school level. This NSF-sponsored initiative's main objective is to educate high school students about cybersecurity through a free summer camp that includes lectures, lab sessions, and free lunch and snacks, focusing on including students from low-income and underrepresented families. It also aims to teach students to recognize fraudulent behavior in malicious apps by exposing them to apps that behave fraudulently.

Goals and Objectives

A cybersecurity summer camp for high school students aims to provide students with a comprehensive introduction to the field of cybersecurity and the potential consequences of cyber-attacks. The main goal of this camp is to expose students to the various career opportunities available in cybersecurity and to educate them on the basics of computer and network security. The session name and its respective learning objectives are shown in Table 1. In addition, the camp provides hands-on experience through labs and applications that allow students to apply their knowledge in a practical setting. By participating in these hands-on activities, students can develop a better understanding of the concepts they are learning and gain valuable skills that can be applied in their future studies or careers. Student-centered learning strategies are effective at enhancing student learning, according to research [5].

Table 1 Session Name and its respective learning Objectives

Session Name	Learning Objectives
Intro to Cybersecurity	• Cybersecurity Importance • Few past and recent Cyber attacks • CIA triad • Threat, vulnerability, attack • Domains of Cybersecurity
Cryptography	• What is Cryptography? • Types of Cryptography • Usage • Real World Examples of Cryptography
Malicious Software	• What is Malware? • Targets of Malware • Malware Attacks Trends • Types of Malware • Prevention/Detection
Cyber-safe Practices	• Cyber Safety (Electronic devices) • Dangers (Cyberbullying, Online Predators, Phishing, Identity theft, etc.)

	• Common mistakes (E.g.: Reusing Passwords, leaving unlocked devices unattended etc.) • Staying Safe (Password Management, Two Factor Authentication, etc.)
Internet Security	• Introduction • Type of Internet attacks (Malware Spread, Sniffing, Ip Spoofing, etc.) • Attacks on TCP (TCP SYN Flooding) • Attacks on DNS • Defense tools (Firewall, Intrusion Detection System etc.)
Web Security	• Intro to world wide web (www) • Elements of Web • Why Web Security? • Malicious URL • Cross-site Scripting (XSS) attack • SQL Injection Attack

Additionally, the camp helps students develop critical thinking, problem-solving, and teamwork skills. These skills are essential for success in the field of cybersecurity and are also transferable to other areas of study and work.

Cybersecurity awareness is essential since it lowers the possibility of assaults and safeguards data. Therefore, it's crucial to comprehend how to defend against viruses and hackers. So, this study aims to educate high school senior and university freshmen students about cybersecurity topics, such as internet security, web security, cryptography, and malware, through a week-long experience. We aim to assist students in discovering and identifying their cybersecurity interests through this experience. Additionally, it gives students a chance to decide whether to pursue a career in this domain. There is a sizable proportion of pupils from economically underprivileged and/or underrepresented racial and ethnic groups in the public schools of the cities of the participating institutes. According to the Ohio Department of Education's School District Report Card, during the 2021–22 academic year, Toledo Public Schools (TPS) had around 71.4% minority enrollment and 86.8% economically disadvantaged families [6]. Black, Hispanic, and multiracial students make up 47.9% of the minority population at Munster High School (Indiana), which has 50%, female students. 17% of the kids qualified for free or reduced meals [7]. Schools, colleges, and universities must comprehend the significance of cybersecurity to better prepare students for the risks associated with the internet. Students can learn to be safe and secure when accessing the internet and using technology.

Research Methodology and Activities

This study used a quasi-experimental approach in which two participant groups—high school seniors and first-year university students—were exposed to early cybersecurity training via various channels. The senior high school students took part in a summer camp where they learned practical cybersecurity skills and gained exposure to them. On the other hand, first-year university students attended lectures on the same subject as part of their curriculum. Before and after the participants were exposed to the education, their attitudes regarding pursuing a career in cybersecurity were compared using the pre- and post-surveys.

Students who attended the summer camp and were seniors in high school and first-year students in college made up the sample population for this study. Being a high school senior or a university freshman and having an interest in technology and cybersecurity were requirements

for participation in the study. Twenty-six high school students attended the summer camp at the University of Toledo and Purdue Northwest University. Roughly 130 students from the University of Toledo attended the lectures as first-year students. For the objectives of this study, a sample size of 130 first-year university students and 26 campers was deemed adequate because it allowed for the collection of valuable data and the analysis of the findings. Due to the small sample size, it's crucial to remember that the conclusions might only apply to some of the more significant populations of high school seniors and first-year university students.

To assess the participants' comprehension of several cybersecurity-related issues. The data were compiled using descriptive statistics, like the mean, to give a broad overview of the participants' comprehension levels. The surveys evaluated participants' knowledge of and attitudes about cybersecurity and covered subjects like phishing, security, and malicious software. In addition, several other interventions, such as hands-on experiments, app development exercises, in-house developed educational apps (aka "*fake*" apps), and an animation-based teaching tool, were employed. Drawing conclusions regarding students' perspectives on cybersecurity and their decision to pursue it as a career depends mainly on the data collected using surveys that were conducted before and after the interventions. Surveys were conducted in a pre/post setting, and the results indicated a positive change in the interest of students in pursuing a career in cybersecurity.

Engaging High School Students in Cybersecurity Learning

The week-long high school summer camp was created to give pupils a practical and exciting cybersecurity education. The students were exposed to cybersecurity-related topics from 9:00 am to 3 pm, including practical lab sessions where they received the required guidance and support to ease their concerns. Schools need more knowledge, resources, and financing to implement cybersecurity education [8]. The high school summer camp's lecture sessions were thorough and covered various cybersecurity-related topics. These topics included cryptography, best practices for online safety, malicious software, AI and ML fundamentals, and security applications. In addition, the students learned about Internet Security and Web Security, two crucial elements of contemporary cybersecurity. The lectures were made to give pupils a strong base of information and abilities. The high school summer camp was created to offer an in-depth and enjoyable opportunity for cybersecurity education. The labs included the Android App Lab, Cryptography Lab, Malware Visualization Lab, Network Lab, Interactive Visualization Lab, Android Malware Lab, and Web Security Lab. Students were allowed to practice the ideas they had acquired in theoretical courses and put them into practice in these labs.

The Android App Lab's hands-on learning experience was a highlight of the high school kids' summer camp. The students used the MIT App Inventor to design various applications they could download and use on their own devices. Students gained a more profound knowledge of using this practical method. Through this practical approach, students gained a greater comprehension of how applications operate and the potential for them to spread malicious software. A "Hello-world" app with a button that talks the message stored within the app, a "To-Do list" app that allows students to store and manage a list of daily tasks, a "Tiny-banking" app that simulates a concise banking system with a default balance of 200 dollars and buttons for withdrawals and deposits, and a game of "Tic-Tac-Toe" are just a few of the applications that students built. Each of these applications allowed students to use their newly acquired knowledge and see how the ideas they learned, in theory, could be used in real-world situations.

Students learned about cryptography's fundamentals through practical exercises at the

Cryptography Lab. Students' understanding of encryption and decryption algorithms was improved by these exercises. Additionally, they discovered the significance of key management and how it helps to protect encrypted data. Additionally, through working on a practical project where they had to encrypt and decrypt a picture, the students had the opportunity to learn how encryption was used in real-world situations. Students now have practical knowledge of how cryptography functions and how it can be applied to safeguard data in the real world. By working on this project, students could understand the significance of cryptography and its function in protecting security. To help students comprehend how networks work and how data is transported over the internet, the Network Lab and Interactive Visualization Lab were created. The Web Security Lab and the Android Malware Lab gave students practical experience identifying and defending against web-based threats and malicious malware. Through these labs, students understood cybersecurity's significance and the crucial role cybersecurity experts play in safeguarding sensitive information.

Students were supervised by skilled professionals who were on hand to assist and guide them as needed during the lab sessions. All students could participate entirely and make the most of the hands-on learning opportunity because of the attentive supervision. Each lab exercise's complete manual was a valuable resource, offering pupils simple, comprehensible directions they could readily follow. Even if they were having difficulty understanding the ideas, these instructions helped students make the most of their classroom instruction and gave them the confidence to complete the exercises. A closing ceremony and certificate presentation were held on the last day of summer camp to honor the diligent work of the participants.

Delivery of Cybersecurity Education to Undergraduate Students

1. **Overview of the lecture schedule:**

The lecture series, which spanned two weeks, was intended to give undergraduate students a thorough understanding of the cybersecurity profession. The subjects discussed included:

- Cryptography
- Malicious software
- Web & Internet Security and Privacy
- Cyber Safety Practices

The target audience included 135 undergraduate students who attended the 80-minute seminars every week on Tuesday and Thursday for two weeks. On Monday, surveys were given out before the lectures to get feedback from the students and determine how well they understood the subject matter. After the second week of classes, these surveys were compiled and examined. Hands-on lab assignments were provided on Blackboard for students to perform independently and without supervision to complement the lecture sessions. With this method, students could put the ideas they had acquired in lectures into practice and further their understanding through hands-on learning.

On Monday, surveys were given out before the lectures to get feedback from the students and determine how well they understood the subject matter. After the second week of classes, these surveys were compiled and examined. Hands-on lab assignments were provided on Blackboard for students to perform independently and without supervision to complement the lecture sessions. With this method, students could put the ideas they had acquired in lectures into practice and further their understanding through hands-on learning. The lecture sessions' goal was to give a thorough understanding of the significant cybersecurity issues and their

applications. Students learned about a wide range of topics, such as:

- **Cryptography**: The first session is on cryptography fundamentals, which cover encryption and decryption algorithms. The pupils could comprehend how to encrypt and decrypt messages and images and the function of cryptography in ensuring data security.
- **Cyber Safety Practices:** This section discussed the value of good cyber hygiene and recommended procedures for online safeguarding private and sensitive data. Students were taught the risks of phishing scams, password security, and other typical issues.
- **Malicious Software**: In this session, students learned about the various kinds of malware and how these programs may infect computers and other devices.
- **Introduction to the Internet:** This section gives a thorough overview of the Internet and its different parts, including the World Wide Web, email, and other widely used programs.
- **Internet Security:** This part discussed the fundamentals of Internet security as well as the different kinds of attacks that can happen. Students gained knowledge of the risks associated with insecure networks, phishing scams, and other typical hazards.
- **Web Security and Privacy Fundamentals:** In this section, students explored the fundamentals of web technologies and how to defend against frequent web-based attacks, including cross-site scripting (XSS) and cross-site request forgery (CSRF). The significance of web application security was also taught to them. In addition, privacy and related concepts were discussed.

2. **Overview of the lab sessions**

The lab sessions were made to be self-paced so that students could finish the tasks when convenient for them. Due to the flexible timetable made possible by this method, all student's various demands and schedules could be met. To ensure they fully grasped the topic before going on to the next exercise, students had the chance to ask any questions or raise any issues regarding the lab exercises during the lecture sessions. The absence of direct supervision throughout the lab sessions allowed the students to hone their independence and problem-solving abilities as they completed each activity. Comprehensive guides with step-by-step instructions for each exercise were also available to help the students throughout the lab sessions. This allowed students to finish the labs on their own time and gave them the opportunity to reference the manual if they ran into any problems or obstacles. The guidebook was a useful tool that empowered pupils to do the activities on their own and with more confidence.

Results

1. **Assessment of Undergraduates' Understanding of Cybersecurity**

This section of the paper's results sought to examine how the University of Toledo's first-year students responded to the cybersecurity lecture sessions. Surveys given out before and after the lectures were used to gather the data. Each survey had ten questions addressing various cybersecurity-related issues, and there were five options for the students to select from for each question. Based on how much respondents agreed or disagreed with the statement, these answers were given a numerical value between 1 and 5. The data gathered from the surveys were presented in this section in a thorough and well-organized manner, including tables and charts to make the findings easy to understand. To ascertain any improvements in the students'

comprehension and awareness of cybersecurity subjects, we examined the responses of the students and compared the findings of the pre-lecture and post-lecture surveys. The influence of the lectures on the student's knowledge and comprehension of the subject was also discussed in this part, along with the students' perspectives and attitudes regarding cybersecurity. We sought to assess the success of the lecture sessions in providing cybersecurity education to first-year students through the analysis of the findings and to pinpoint any areas where program enhancements might be made in the future.

There were ten questions with five different options, from "Strongly Agree" to "Strongly Disagree," for each one. Based on each respondent's response to each question and their degree of agreement or disagreement with the question, 1 to 5 as shown in *Table 2* was assigned to each choice, transforming the reactions into a numerical representation. A graphical representation of the average value for each question in the pre-and post-surveys is provided as follows.

Table 2 Mapping categorical data to numerical values

Strongly disagree	1
Somewhat disagree	2
Neither disagree nor agree	3
Somewhat agree	4
Strongly agree	5

Except for questions 1 and 9 in Figure 1, the results show that the average value of the questions in the post-survey was higher than in the pre-survey in all survey results as shown in Figure 2 and Figure 3, demonstrating that the students had a more excellent knowledge of the topics

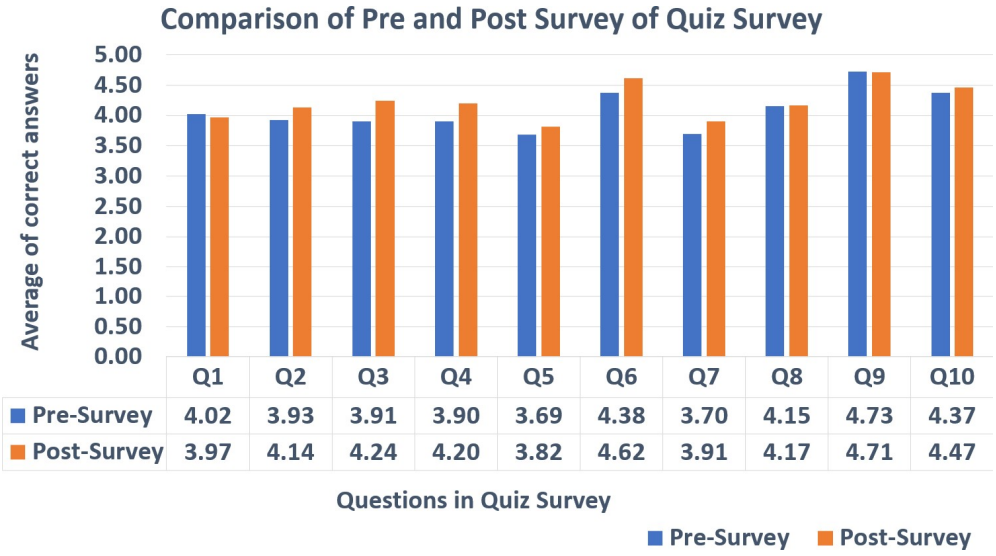

Figure 1 Comparison of pre and post-survey results of Quiz Survey

introduced during the lectures and lab activities. The survey questions for the Quiz Survey, Phishing-Chat App Survey, and Phishing-Facebook Survey are shown in Table 2, Table 3, and Table 4 respectively. The survey findings indicate that the lecture sessions had a beneficial effect on the student's comprehension of the subjects in cybersecurity. Following the lecture

sessions, the students appeared to have improved their knowledge and understanding of the subject, as evidenced by the rise in the average value of each question in the post-survey compared to the pre-survey. This may be ascribed to the thorough lecture materials and practical lab exercises that were made available to the students, which helped to reinforce the ideas and provide them with hands-on experience using the knowledge acquired. The findings support the idea that providing cybersecurity education to undergrad students can significantly affect their comprehension of and readiness for the sector.

Table 2 Questions of Quiz Survey

S. No.	Questions of Quiz Survey
Q1	You should download any mobile application only from legitimate sources such as Play Store
Q2	After the app has been downloaded, you must grant all the permissions that it has asked for the proper functioning of the app.
Q3	You should grant "Phone" permissions to an app that is used to click pictures
Q4	Media on your smartphone is secure as you only hand over your phone to those you trust.
Q5	A mobile app can share your data on an external website without your consent.
Q6	It's fine to download email attachments even if the email app cautions you with a warning message.
Q7	Educational apps can be granted all the permissions such as the Internet, Access to media storage, and location.
Q8	Antivirus software is a must for all computers.
Q9	Everything you read on the internet is true
Q10	You should not share your personal details with someone you have met online.

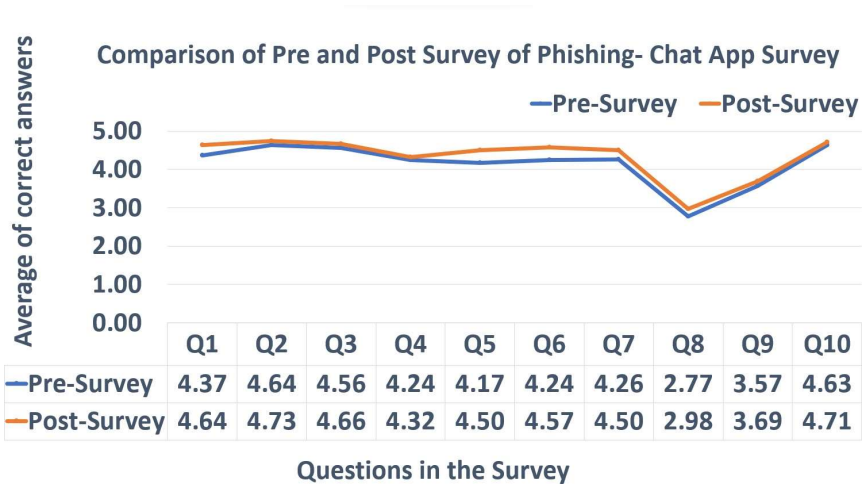

Figure 2 Comparison of Pre and Post Survey of Phishing- ChatApp Survey

Table 3 Questions in Phishing-Chat App Survey

S. No.	Questions in the Survey
Q1	Every text you get on your phone comes from people you know.
Q2	You can trust a text or email message that claims to have a gift card for you.
Q3	Clicking on the links in a text message or e-mail from an unknown sender is not unsafe.
Q4	Unsafe and unsecured URLs do not exist. For example, http://amazonsurprises.com/ and https://amazonsurprises.com/ are the same.

Q5	The safest way to save all your personal information, including university data, is by saving it to notes on your mobile phone.
Q6	You can be a victim of Phishing if you're not careful when using your social media accounts on public devices.
Q7	The use of "Public WIFI" is secure and inexpensive since its free to use.
Q8	You can save yourself from becoming a victim of Phishing by using complex alphanumeric passwords.
Q9	Phishing attacks can only occur when you click on a malicious link in your mobile browser.
Q10	Responding to emails that claim you've earned a reward or inherited wealth will make it easier for you to earn money.

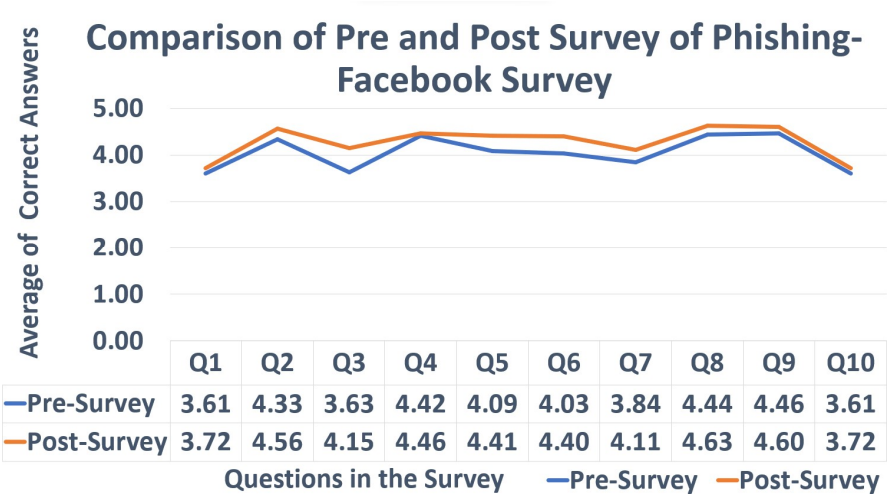

Figure 3 Comparison of Pre and Post Survey of Phishing Facebook Survey

Table 4 Questions in Phishing-Facebook Survey

S. No.	Questions in the Survey
Q1	Apart from "App Store" and "Play Store," any mobile app can be updated from other websites on the Internet.
Q2	Any mobile app that looks familiar or similar to a well-known app is safe to trust.
Q3	I know what cyber threats are and what phishing is all about.
Q4	Hackers target for phishing attacks at both common man and highly reputed organizations.
Q5	Phishing attacks can only occur on mobile financial transaction apps, such as banking.
Q6	Phishing attacks are intended to steal confidential personal data.
Q7	One may avoid being a victim of phishing by following specific guidelines.
Q8	Never be suspicious about emails asking for your personal information.
Q9	Social media can also be a platform for phishing attacks.
Q10	A third party cannot access the details of my personal social media account without my permission.

2. Assessing High School Student Interest in Cybersecurity as a Future Career

a. Choosing Cybersecurity as a career

The rise in the percentage of students who only partially disagreed that they should pursue a career in cybersecurity is a sign that the lectures and hands-on labs have successfully promoted the profession as shown in Figure 4. The decline in the percentage of students who partially

disagreed, and the unsure students may suggest that the program has assisted in resolving any

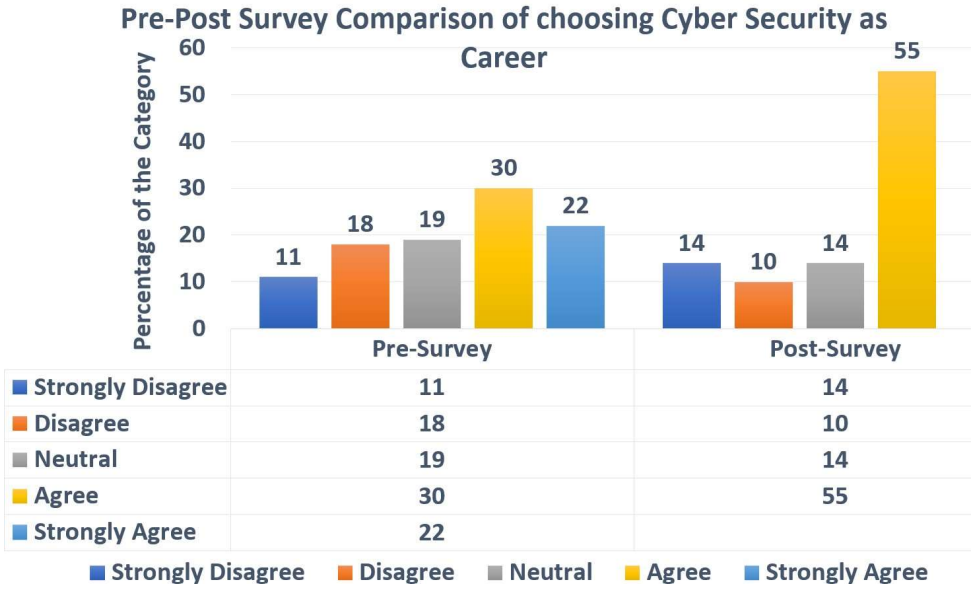

Figure 4 Pre-Post Survey Comparison of Choosing Cybersecurity as a Career

issues or worries some students may have had. It is necessary to recognize the increased number of strongly objected students, and this implies that there might be obstacles keeping sure students from considering cybersecurity as a career. These elements could be related to how the industry is viewed, a lack of role models, or ignorance of career options in cybersecurity. Consequently, it might be required to investigate other approaches to overcome these obstacles and boost interest and confidence in the area. The findings indicate the program's success in raising awareness of and interest in cybersecurity as a career. However, there is still potential for improvement to persuade more students to consider this field.

b. Changes in Cybersecurity Knowledge of High School Students

The poll's findings in ***Figure 5*** taken before and after the lectures on cybersecurity point to a significant improvement in the student's knowledge of the topic. According to the chart's research, from 0% in the pre-survey to 8.7% in the post-survey, more students now have advanced cybersecurity knowledge. On the other hand, from 46.75% in the pre-survey to 0% in the post-survey, the proportion of pupils with novice knowledge decreased. It is interesting to see that more students now have intermediate knowledge of cybersecurity, which suggests that the lecture sessions, interactive games like Kahoot, and hands-on exercises allowed them to comprehend the subject better. Also, the games played following lunch helped the youngsters perform better. Overall, the student's cybersecurity knowledge was improved due to the lectures, games, and practical exercises. The survey's findings imply that students are now much more interested in and aware of cybersecurity as a potential career. These results emphasize the need for comparable programs to increase student understanding of cybersecurity and inspire them to pursue professions in this industry.

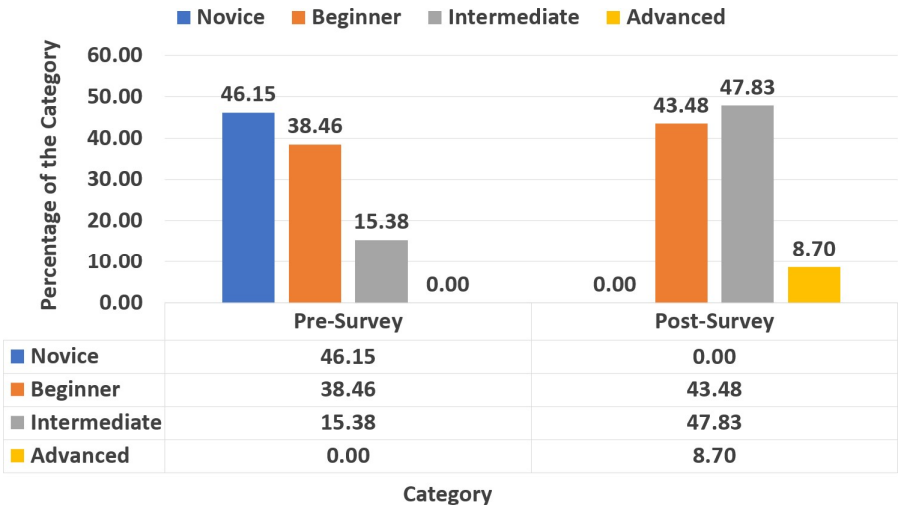

Figure 5 Pre- and Post-Comparison of knowledge rating on Cybersecurity

Conclusions

The findings indicate a favorable change in students' perceptions of cybersecurity as a potential career. The percentage of students interested in a career in cybersecurity increased significantly, while the proportion of unsure pupils decreased. The rate of students who strongly disagree with a career in cybersecurity has also increased, so it's important to note that there is still some hesitation among students to pursue this field. Overall, the survey results show that improving students' knowledge and interest in cybersecurity through the summer camp and undergraduate education was successful. Yet, it is essential to keep working to dispel students' misunderstandings and raise awareness of the advantages of choosing cybersecurity as a career.

Acknowledgement

This material is based upon the work supported by the United States National Science Foundation under Grant No. 1903419 and 1903423 through the Security and Trustworthy Cyberspace Education (SaTC: EDU) program. Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. This study was approved by the Institutional Review Board (IRB) at Purdue University Northwest and the University of Toledo under protocol numbers IRB-2020-1119 and IRB-301407-UT, respectively.

References

[1]. Khalid, F. (2017). Understanding University Students‘ Use of Facebook for Collaborative Learning, International Journal of Information and Education Technology, Vol. 7, No. 8, August 2017, 595-600

[2]. Zakaria, N. & Khalid, F. (2016). The Benefits and Constraints of the Use of Information and Communication Technology (ICT) in Teaching Mathematics, Creative Education, 7, 1537- 1544. http://dx.doi.org/10.4236/ce.2016.711158

[3]. Oxford University Press. (2014). Oxford Online Dictionary. Oxford: Oxford University Press. [Online]. Available: http://www.oxforddictionaries.com/definition/english/Cybersecurity

[4]. DHS. (2014). A glossary of common cybersecurity terminology. National Initiative for

Cybersecurity Careers and Studies: Department of Homeland Security. [Online]. Available: http://niccs.uscert.gov/glossary

[5]. Jaccheri, F. Q. (n.d.). Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction.

[6]. N. Ahmad, U. A. Mokhtar, W. Fariza Paizi Fauzi, Z. A. Othman, Y. Hakim Yeop and S. N. Huda Sheikh Abdullah, "Cyber Security Situational Awareness among Parents," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-3, doi: 10.1109/CR.2018.8626830.

[7]. N. Debra, P. Karen, "The Urgency for Cybersecurity Education: The Impact of Early College Innovation in Hawaii Rural Communities"

[8]. Impact of Smartphone-Based Interactive Learning Modules on Cybersecurity Learning at the High-School Level

[9]. Bhuyan, J., Wu, F., Thomas, C. et al. Aerial Drone: an Effective Tool to Teach Information Technology and Cybersecurity through Project Based Learning to Minority High School Students in the U.S.. TechTrends 64, 899–910 (2020). https://doi.org/10.1007/s11528-020-00502-7

[10]. G. O'Neill, T. McMahon "Student-Centered Learning: What does it mean for students and lecturers", University of College Dublin. [Online]. Available: http://www.aishe.org/readings/2005- 1/oneill-mcmahon-Tues_19th_Oct_SCL.html

[11]. Education, O. D. (2022). Ohio School Report Cards - Toledo City District Details.

[12]. News, U. (n.d.). https://www.usnews.com/education/best-high-schools/indiana/districts/school-town-of-munster/munster-high-school-7312.