2023 Annual Conference & Exposition
Baltimore Convention Center, MD | June 25 - 28, 2023
The Harbor of Engineering Education for 130 Years
ASEE
Paper ID #39771

Evaluating the Impact of a Multimodal Cybersecurity Education Approach on High School Student Cybersecurity Learning

Xiaoli Yang
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.

SaiSuma Sudha
Sai Sushmitha Sudha

Evaluating the impact of a multimodal cybersecurity education approach on high school student cybersecurity learning

Sai Suma Sudha[1], Sai Sushmitha Sudha[1], Ahmad Y Javaid[1], Quamar Niyaz[2], Xiaoli Yang[3]

[1]EECS Department, The University of Toledo, Toledo, OH, United States

[2]ECE Department, Purdue University Northwest, Hammond, IN, United States

[3]CS Department, Fairfield University, Fairfield, CT, United States

{saisuma.sudha, saisushmitha.sudha, ahmad.javaid}@utoledo.edu, qniyaz@pnw.edu, xyang@fairfiled.edu

Introduction

The need for cybersecurity is growing as we become more dependent on digital tools and programs to run our daily lives, including the sharing, and storing of personal data. Due to the pervasive use of technology and the rise in cyber threats, people must be equipped with the information and skills necessary to defend themselves and their devices from cyberattacks. This is particularly crucial for high school students who are growing up in a digital age and will soon be entering the profession. According to research reports, a successful security awareness program is one of the critical milestones in boosting and bolstering cybersecurity [1]. For students to start thinking about security as a requirement before developing any system, security-related concepts must be incorporated into the existing courses. The rise in cyberattacks shows that the conventional methods of education and awareness still need to be improved to develop the required cybersecurity competencies [2]. This project aims to increase the understanding and abilities of high school students in cyber security. The primary goal of this project is to give students a complete understanding of cybersecurity by using an interactive visualization tool, explaining cybersecurity through lectures, lab/experimental sessions, and smartphone app development exercises. To improve high school students' understanding of cybersecurity, Purdue University Northwest and the University of Toledo conducted a week-long summer camp, collected relevant data, and analyzed the results to see the impact.

Related Work

Numerous computer-based instructional techniques are now possible due to the growth of technologies, fast connections, and the widespread use of mobile devices. As a result, cybersecurity education is in dire need of an innovative curriculum and teaching approaches. Game-based learning is one of the emergent and quickly evolving types of computer-based learning. Creating cloud services and ready-to-use cybersecurity training courses, with a focus on teaching and training cybersecurity algorithms is essential [3]. Providing a virtual lab offers a practical learning environment is a crucial step, to enable thousands of students to access online cybersecurity education [4]. A visual lab provides students with a simulated environment where they can gain hands-on experience with cybersecurity tools and techniques without any physical equipment. Establishing a virtualized learning environment is an effective approach for cybersecurity teaching [5]. The use of game-based learning in cybersecurity camps can be an

effective way to introduce students to key topics in cybersecurity [6]. As technology becomes more pervasive, helping students understand the importance of cybersecurity in their careers is crucial for preparing them for the demands of the modern workforce[7]. A cybersecurity awareness program that utilizes a game-like learning environment can be an effective way to engage students and promote cybersecurity best practices [8].

Goal and Objective

This project aims to expand high school students' knowledge about cybersecurity. Therefore, we offered a free summer camp whose main goal was to educate high school students on the necessity of cybersecurity and the many cyberattacks they can come across in daily life, like phishing, scareware, and ransomware. Students attended classes on campus five days a week from 9:00 am to 3:00 pm. There was a lunch break in between. The morning sessions began with a straightforward explanation of cybersecurity principles, followed by interactive lab sessions in the afternoon, Figure 1 shows the schedule of the summer camp that took place. Through these lab sessions, students also gained a strong understanding of how phishing, scareware, and ransomware operate in the real world. Students learned how cyber-attacks might occur through this. Utilizing MIT App Inventor, students also learned how to design applications. To accomplish the goals of our study, we completed a survey that included 6 pre-surveys and 6 post-surveys, which we then distributed to the students. The findings of our survey show that the summer camp was successful in teaching cybersecurity to students irrespective of gender, race, or previous background in the domain.

Day	Agenda Topic
Day 1	Intro to Cybersecurity
	Android Overview
	Android App Lab 1
Day 2	Cryptography
	Cyber Safety Practices
	Cryptography Lab
	Android App Lab 2
Day 3	Malicious Software
	Malware Visualization Lab
	AI/ML Basics and Applications to Security
	Android App Lab 3
Day 4	Intro to Internet
	Internet Security
	Network Lab
	Interactive Visualization Lab
	Android Malware Lab
Day 5	Basics of Web Security
	Web Security Lab
	Closing and Certificate Distribution

Figure 1 Cybersecurity summer camp schedule

Research Methodology and Activities

30 students aged 14 to 17 of all races attended the summer camp (like Asian, white, Black or African American, etc.) We engaged the students in several activities to help them learn about cybersecurity, such as (i) Interactive visualization tool, (ii) MIT App Inventor (for smartphone app development), (iii) Lecture sessions with thorough explanations, (iv) lab/hands-on sessions, and (v) exposure to various types of malwares.

1. Interactive visualization tool

Tools for interactive visualization are an efficient approach to include students and provide them with a practical introduction to cyber security. These resources can aid students in understanding sophisticated security methods and concepts. The interactive visualization tool was created using the Unity gaming engine, a platform for game-based programming [9]. Students gained practical knowledge using this application in cryptography, malware, network security, and web security modules of cybersecurity.

Figure 2 shows the menu screen of the visualization tool. Each module had four stages such as Information, Interaction, Explanation and Assessment [10]. Figure 3 shows the four stages of Caesar Cipher of Cryptography module. The modules description was provided during the information stage. To understand the module, the interaction stage offered an interactive sample. The interactive example was explained at the explanation stage. In assessment stage a quiz is included in each module to assess the student's knowledge of the content.

Figure 2 Menu of visualization tool

Figure 3 Shows the four stages of each Caesar Cipher

2. MIT App Inventor

An integrated development environment for web applications called MIT App Inventor was first made available by Google and is now maintained by the Massachusetts Institute of Technology (MIT). The blocks-based programming environment MIT App Inventor allows anyone to create mobile apps for Android smartphones, even those without coding experience. A drag-and-drop interface offered by App Inventor makes it simple to design apps. In MIT App Inventor, the elements of an app are represented as blocks, and an app is created by arranging the blocks in the correct order. So, the students don't need any technical knowledge. Students created different applications such as Tic-Tac-Toe, Tiny banking, and To-Do-List. When building the apps, students found them incredibly simple and enjoyable.

3. Lecture sessions

The primary goal of these lectures is to teach the students about cybersecurity modules and how to develop a cybersecurity attitude, which is crucial in today's society. Students got clear understanding on the topics of cryptography, malware, network security, web security and internet security through these explanations. The student's doubts were clarified throughout the lectures as well. The students were also given information on the fundamentals of AI/ML and security applications. The lectures were very informative and used examples from the real world to convey the topics. It was discussed in detail how cybersecurity works on a fundamental level. Students were also aware of issues like password security and online privacy.

4. Lab sessions

Students had the opportunity to use the cybersecurity modules practically during lab sessions. Students used MIT App Inventor to develop applications, and they worked on the applications enthusiastically. Through these lab sessions, they had hands-on experience with data encryption and decryption, network security, different malware forms they would encounter daily, and website security. They were given several sample examples to help them understand these issues practically. Students were aware of the issues that cybercriminals can cause.

5. Exposure to various types of malware

Students were exposed to numerous forms of malware, which helped them comprehend the consequences of cyber threats in the real world and develop the critical thinking abilities needed to recognize and keep away from them. To help students comprehend how different varieties of malware will be encountered by them daily, they were given a type of malware app and some malicious websites. We have used Fake WhatsApp and Fake Facebook app for the students and gave the explanations clearly.

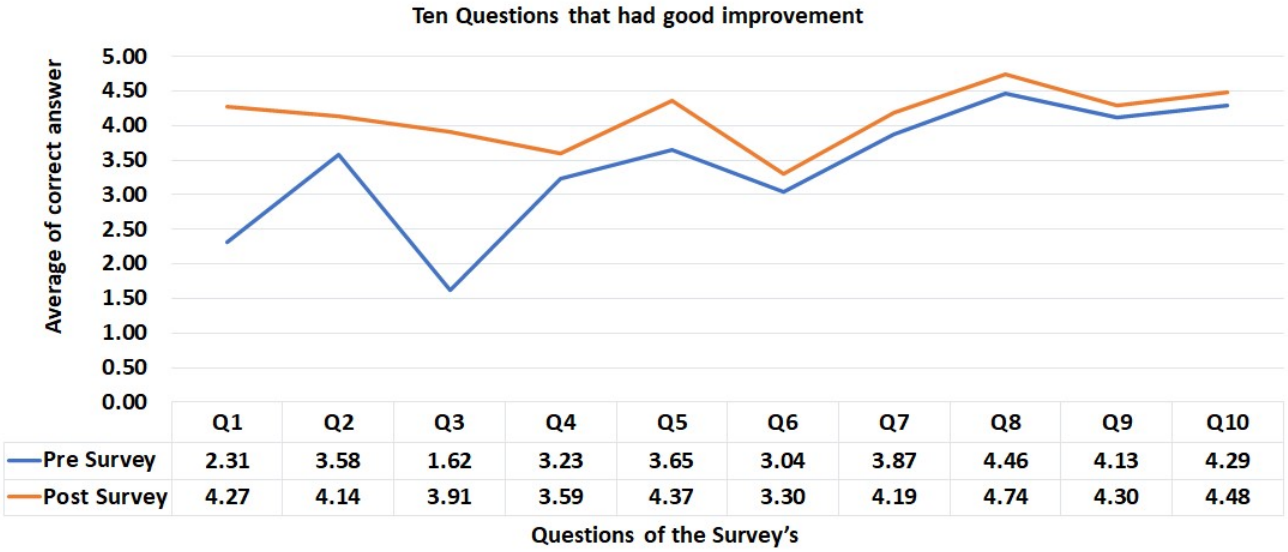
The research questions used during the summer camp are listed below.

1. What curriculum components are most effective in teaching the content?
    a. What are the characteristics of each module that interest students?
    b. Can these characteristics be employed to make other modules more interesting?
2. How effective are interactive animated visualization modules more interesting?
    a. Are the unique differences based on gender and/or race?
    b. Does student perception of cybersecurity concepts improve?

Results

We have collected surveys before and after each session to determine the students' knowledge of the cybersecurity principles taught. Students who attended the University of Toledo and Purdue University Northwest summer camps in 2022 are surveyed. 30 students were subjected to almost 12 surveys, including 6 pre- and 6 post-surveys. From the topics of Cryptography, Malicious and web security, 10 best survey questions that had good improvement were taken and also questions that need an improvement were also taken. So, that we can improve our materials and the explanations for the further camps to give clear understanding to the students. Figure 4 shows the result of survey questions that had improvement. Survey questions on web security, malicious, and cryptography were chosen because of their high scores. And the responses to these questions were presented. Figure 5 shows the questions that had improvement and Figure 6 shows the questions that need an improvement. The results were calculated based on five options available: strongly agree (5), agree (4), neither agree nor disagree (3), disagree (2), and strongly disagree (1). We selected the survey questions that the students gave incorrect answers from the survey's topics of Cryptography, Malicious and web security. We provided the information for the questions that

want improvement. Figure 7 shows the results of the survey questions that need improvement.



	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Pre Survey	2.31	3.58	1.62	3.23	3.65	3.04	3.87	4.46	4.13	4.29
Post Survey	4.27	4.14	3.91	3.59	4.37	3.30	4.19	4.74	4.30	4.48

Figure 4 Result of 10 questions that had good improvement.

QNo	QUESTIONS THAT HAD IMPROVEMENT
Q1	I understand what is cryptography.
Q2	I don't think I need to hide my information when I am sending a text to a friend.
Q3	I have heard of terms like RSA, AES, etc before.
Q4	Does the recent cryptography algorithms have threat from quantum computing?
Q5	I know what cyber threats are and what phishing is all about.
Q6	Apart from "App Store" and "Play Store," any mobile app can be updated from other websites on the Internet
Q7	Phishing attacks are intended to steal confidential personal data.
Q8	Unsafe and unsecured URLs do not exist. For example, http://amazonsurprises.com/ and https://amazonsurprises.com/ are the same.
Q9	You can be a victim of Phishing if you're not careful when using your social media accounts on public devices.
Q10	The use of "Public WIFI" is secure and inexpensive since its free to use.

Figure 5 Questions that had improvement

QNo	QUESTIONS THAT NEED IMPROVEMENT
Q1	I have purchased crypto-currency and know the concepts they are based on
Q2	One may avoid being a victim of phishing by following specific guidelines
Q3	Any mobile app that looks familiar or similar to a well-known app is safe to trust.
Q4	Phishing attacks can only occur on mobile financial transaction apps, such as banking.
Q5	Social media can also be a platform for phishing attacks.

Figure 6 Questions that need improvement

We also gender-specifically assessed the survey data, and the findings indicate that males have made significant progress in understanding Internet security and cybersecurity. In Figure 8 the results of Pre-Post Survey comparison of Internet security based on gender is shown. Results of

the cybersecurity of pre-post survey based on gender is shown in Figure 9. I created a bar chart to compare the cybersecurity pre and post-survey results since I want to present the information in various formats.

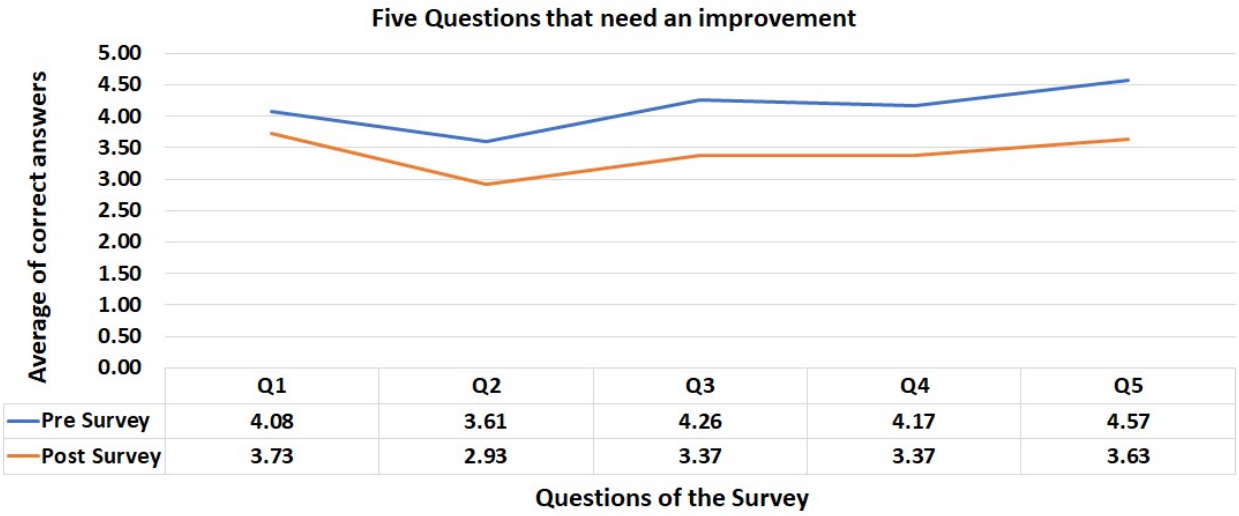


Figure 7 Results of the survey questions that need improvement.

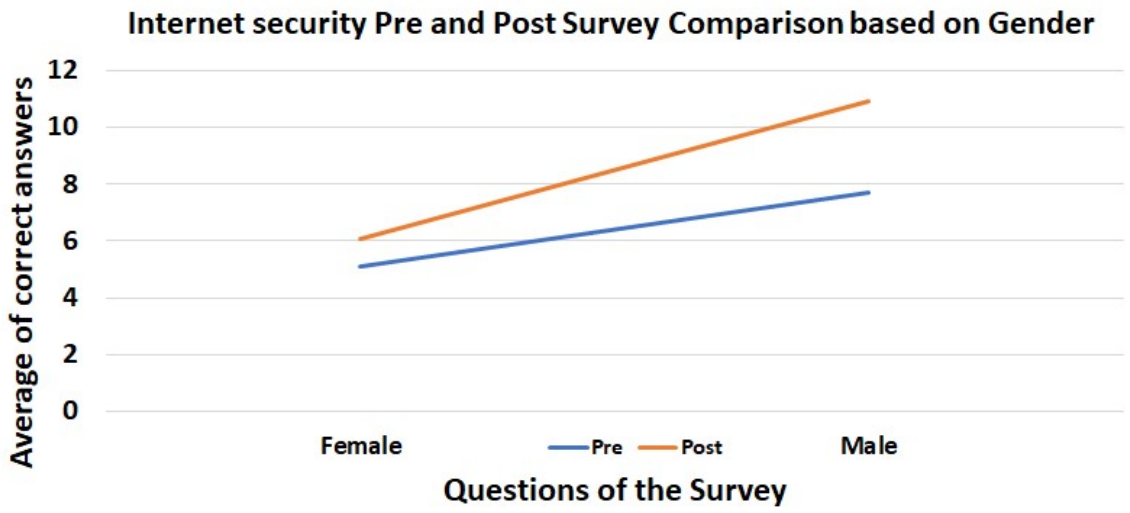


Figure 8 Results of Pre-Post Survey comparison of Internet security based on gender

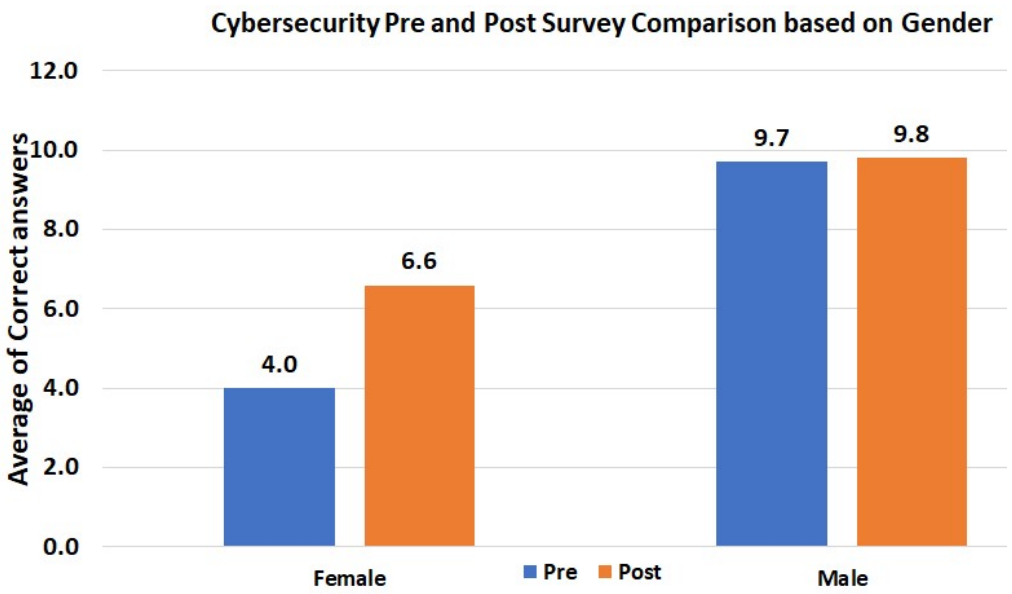


Figure 9 Results of Pre-Post Survey comparison of Cybersecurity based on gender.

Data for cybersecurity is categorical, and responses to the survey were converted to a score of 0 for incorrect answers and 1 for correct ones. The results are then determined by comparing the means of the genders for the pre-survey and post-survey. We assessed the student's skill level before and after the summer camp, and the results show that there is a very good improvement in the student's cybersecurity skill level. The results in Figure 10 gives us a clear understanding about the student's cybersecurity skill level. The results of the pre-survey and post-survey question, "Please rate your knowledge of cybersecurity," was utilized to determine the level of cybersecurity skill.

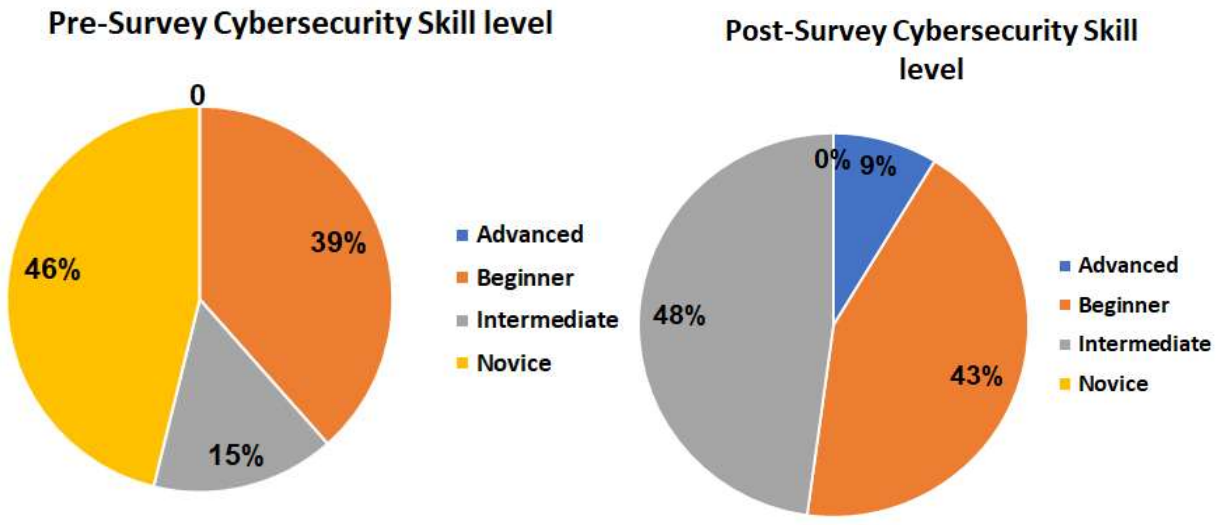


Figure 10 Results of Cybersecurity Skill level

We also assessed on the students question of No. of Programming Languages known for the students, before and after the summer camp. The results shows that students got a good idea on this too. The results are shown in Figure 11.

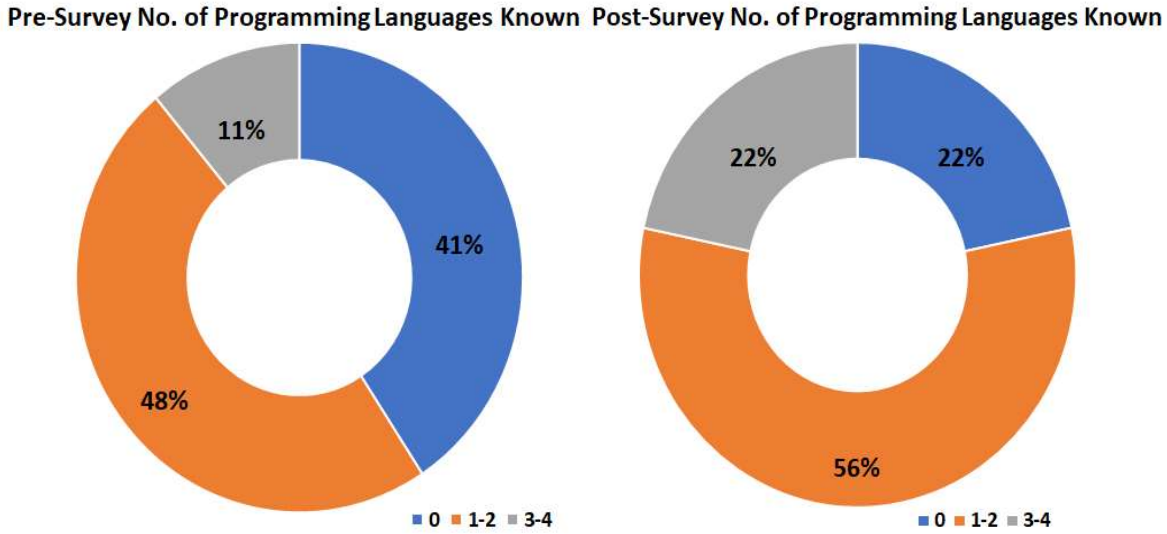


Figure 11 Results of No. of Programming Languages Known.

Conclusions

The objective is to determine whether this method successfully increases students' comprehension of and familiarity with cybersecurity ideas and their capacity to apply these concepts in practical settings. The survey's findings indicate that students are becoming more aware of cybersecurity. We hosted high school students' summer camps at Purdue University Northwest and the University of Toledo in 2021 and 2022. An analysis of the pre-and post-survey results reveals that students were impressed and ultimately impacted how they comprehended. The students who attended the summer camp provided the survey data. The results demonstrate improved web security, malicious software, and cryptography. And for the topics that require improvement, we'll focus on enhancing the supporting information and explanations for better outcomes.

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]. Y. Peker, L. Ray. Online Cybersecurity Awareness Modules for college and High school Students.

[2]. H. Qusa, J. Tarazi. Cyber-Hero: A Gamification framework for Cyber Security Awareness for High School Students.

[3]. C. Willems and C. Meinel. Tele-Lab IT-Security: An Architecture for an Online Virtual IT Security Lab. International Journal of Online Engineering.

[4]. J. Haag , H. Vranken and M. van Eekelen. A virtual classroom for cybersecurity education.

[5]. J. Son , C. Irrechukwu and P. Fitzgibbons. Virtual lab for online cyber security education. Communications of the IIMA.

[6]. G. Jin, and M. Tu, and K. Tae-Hoon and H. Justin and W. Jonathan. Game based Cybersecurity Training for High School Students.

[7]. 5 Cybersecurity programs for High School Students. https://www.indeed.com/career-advice/career-development/cyber-security-programs-for-high-school-students. Published: October 18, 2021.

[8]. L. Chengcheng and K. Rucha. Cybersecurity Education through Gamification – the CTF Approach

[9]. Unity. (2022)Unity scenes. Available: https://docs.unity3d.com/2022.1/Documentation/Manual/CreatingScenes.html Accessed: November 7, 2022.

[10]. Gabriel A Castro Aguayo, Abel R Angulo, Sai S Sudha, Jyothirmai Kothakapu, Quamar Niyaz, Xiaoli Yang and Ahmad Y Javaid. Changes in High-School Student Attitude and Perception Towards Cybersecurity Through the Use of an Interactive Animated Visualization Tool.

Appendix

Appendix A: Survey Procedure

The surveys were conducted to the summer camp students using an online survey platform. Students were provided with a unique link to the survey, which they could complete at their convenience. The survey consisted of multiple-choice and question-answer type designed to assess the student's knowledge and behaviors related to cybersecurity. In total, 6 pre-surveys and 6 post-surveys were conducted to the students.

Appendix B: Data Analysis

The surveys were conducted to assess students' knowledge and attitude regarding various topics related to ELASS, Cryptography, Cybersecurity, Internet Security, Malicious Software and Web Security. To collect data, multiple-choice questions, closed-ended questions, and question- answer type was used, where students were asked to select the option that best fit their response. In some questions, a Likert scale is used to measure the strength of their agreement or disagreement with a statement. The Likert scale ranged from "strongly agree" to "strongly disagree", with a numerical value assigned to each response option (e.g., strongly agree (5), agree (4), neither agree nor disagree (3), disagree (2), and strongly disagree (1)).

In addition to multiple-choice questions and Likert scales, some questions in the survey had specific, predetermined answers. These questions required students to provide a specific response and were graded as correct or incorrect. Correct answers were given a score of 1, while incorrect answers were given a score of 0.

The questions in the surveys helped to collect data, which can facilitate data analysis and helped to identify the areas where further education or training may be needed.

Appendix C: Data Presentation

Once the data collected was analyzed, created charts that could effectively illustrate the key findings. In particular, the data was used to compare the pre-survey and post-survey results to identify the changes in the student's knowledge on various topics covered in the survey. The charts that were created included, questions with good improvement, questions that need to be improved, cybersecurity skill level, etc. The use of charts to present the survey data helped to highlight the results of the summer camp.