Impact of Smartphone-Based Interactive Learning Modules on Cybersecurity Learning at the High-School Level

Sai Sushmitha Sudha*, Jyothi Priyanka Bandreddi*, Laxmi Mounika Podila*, Ramesh Govindula†, Austin Richardson†, Quamar Niyaz†, Xiaoli Yang‡, and Ahmad Y Javaid*, *Senior Member, IEEE*
*EECS Department, The University of Toledo, Toledo, OH 43560 USA
†ECE Department, Purdue University Northwest, Hammond, IN 46323 USA
‡CS Department, Fairfield, CT 06824 USA
{ssudha2, jbandre, lpodila, ahmad.javaid}@utoledo.edu, {rgovindu, richa366, qniyaz}@pnw.edu, xyang@fairfiled.edu

***Abstract*—The increasing use of computer technologies to perform everyday activities simplifies living, but brings the underlying cybersecurity concern to the fore. Due to the accessibility of smartphones, many teenagers are "online" for significant hours in a day. Many middle and high school students have been victims of a cybercrime through online activities. Additionally, various incidents of Internet fraud have been reported where teenagers are persuaded to buy games, music, and videos without realizing they are falling for a scam or disclosing their credit card information. Studies have shown that implementing a successful security awareness camp is crucial in boosting cybersecurity and attracting talent to this domain. This paper discusses our efforts on creating smartphone apps in the context of cybersecurity to encourage safe use of apps and raise awareness among teenagers. The strategy used is to develop apps with the intention of closing security gaps. By doing this, teenagers gain a wealth of information about cybersecurity. This work aims to develop students' problem-solving skills and create a cybersecurity mindset for dealing with real-world cybersecurity-related problems such as malware or phishing assaults and to promote interest in cybersecurity careers among high school students utilizing smartphone-based interactive learning modules. We also examine gender-specific patterns and evaluate whether students' cybersecurity problem-solving skills have improved due to this novel intervention.**

***Index Terms*—cybersecurity, problem-solving skills, interactive learning modules, cybercrimes**

I. Introduction

The world has become a globally interconnected community due to the swift growth of science and technology. However, the increasing potential of cybersecurity frauds and cybercrimes is no less than an Achilles heel of this development. Hacking, spamming, and phishing are just a few popular examples. The Identity Theft Resource Center® (ITRC) reported 474 public data intrusions in the 2022 Q3, up 15% from 2022 Q2 [1]. The rising number of cybercrime incidents outpacing the human resources available to combat them also indicates that there is a significant cybersecurity skill shortage [2]. Although a lot of attempts are being made to increase cybersecurity awareness among high school kids, cybercrimes have become a significant issue at the high school level. Cybersecurity exploits have increased due to people relying on smartphone apps for daily tasks. Since these risks seem benign app features, it becomes challenging for school students to recognize their significance and true nature [2]. They need to be taught to detect fraudulent behavior in malware apps by introducing them to apps that behave fraudulently.

To reinforce cyber-safety procedures and instill a cybersecurity attitude in pupils from an early age, there is a need for a uniform curriculum for cybersecurity education at the high school level. Since cybersecurity is a very hands-on field, it is essential to instruct and inspire students through real-world, hands-on experiments employing various tools and approaches. Additionally, students must learn how to create cyber-secure apps and comprehend safe online behavior. Currently, there are more mobile devices than people on the planet - approximately 8.3+ billion, according to estimates based on active mobile subscriptions. An all-time high in demand exists for smartphones. For teenagers, apps help finish school tasks and educational research resources. Many teens have created innovative and entertaining apps for safety, gaming, news, and entertainment, primarily for smartphones and tablet usage.

This work aims to impart knowledge on mobile app development skills and the safe use of these apps while maintaining a strong emphasis on cybersecurity and related theories. Kids who use smartphones and are interested in their features will undoubtedly be attracted to the development of an application [3]. The kids will learn to program and create a mobile application during this process, introducing them to programming and opening up the possibility of becoming a mobile app developer as a career in the future. Kids also become aware of the program's potential security flaws by learning the security concepts early in the development process [4]. Although all citizens should be concerned about the increase in cyberattacks, the bigger issue is the shortage of cybersecurity experts [5]. Teens can study mobile application development with the help of this work, and be potentially motivated to pursue a career in the cybersecurity domain, making them more valuable by increasing the number of cybersecurity specialists the nation needs [3].

The paper demonstrates the idea of developing mobile ap-

plications while keeping security in mind. We discuss creation of mobile apps using the platform "App Inventor" and use the emulator "Anbox" to run them. App Inventor, a platform for block-based coding and a visual programming environment, enables the creation of functional apps and was created by MIT (Massachusetts Institute of Technology). Unlike Anbox, which runs the Android operating system inside a container, isolates hardware access, and merges core system functions into a GNU/Linux based system. It's simple for a student to understand the outline of a mobile application when they start learning and using the App Inventor. It also plants the seeds of curiosity and excitement to construct more applications. Application development focuses on adding security to the application, such as encrypting data transported over wireless networks and requiring authentication.

The rest of the paper is organized into five sections. Section II discusses recent and relevant works in this domain. Section III briefly summarizes the methodology followed for this research and the overall approach taken to collect and analyze data. Section IV is dedicated to discussing the apps that were created to emulate the actions of malicious apps, as well as smartphone app development exercises that were built using an open-source, block-programming-based platform known as MIT App Inventor. We summarize the steps for creating Android mobile apps from scratch, from design through deployment to an Android device (or an Android emulator), with thorough explanation of each step. We use the open-source Anbox Android emulator for running the apps on an emulated smartphone. Section V presents the data collection and analysis results indicating that the developed modules successfully provided cybersecurity education to high school students and had a positive impact. The paper is then concluded in Section VI.

II. Related Work

It is common knowledge today that security is crucial in this digital age, and regular news on cyber attacks and data breaches removes doubts about absolute data protection and privacy. Information security encompasses the methodologies and procedures created and used to protect electronic and other private, sensitive, and confidential data from unauthorized access, disclosure, modification, misuse, disruption, and destruction [6]. This contrasts with the umbrella term of cybersecurity, which also includes, among others, defending programs, networks, and systems from electronic attacks. These attacks usually point to changing, destroying, or accessing sensitive information and systems [7]. While network security is considered to stem out of cybersecurity, it is the procedure of taking preventive and physical measures of software and hardware to protect the network infrastructure underlying from illegal access, modification, destruction, malfunction, or improper disclosure by creating a secure platform for users, computers, and programs to put their authorized critical functions within a secured environment [8]. All of the above implies that there has been a paradigm shift in how these areas were viewed in terms of education in the past. New approaches and modern pedagogy methods need to be utilized to enhance education in the cybersecurity domain.

Smartphone use is widespread in society, and malware writers have utilized them as both an in-between target and a victim. The Android platform has created an environment for geeks, hackers, enthusiasts, consumers, and businesses interested in modern toys and charmed not only by their practicality and ease of use but also by their openness and sense of community [9]. Android's pervasive nature and popularity have made it a target for malware writers and cyber criminals, just like the popularity and behavior of Windows made it a target [9]. Contrary to popular belief, a platform can be open source or proprietary to become a target. Whether the platform's popularity or susceptibility to subversion and manipulation made it a target for hackers and attackers is debatable. These additional points must be clarified to students to change the popular and incorrect belief that certain platforms are more secure than others. This will help develop a better security mindset and teach students to exercise caution in using any technology.

Through games, high school students were given an immersive, learner-centered cybersecurity training experience. This method effectively teaches students from different backgrounds real cybersecurity skills [10]. According to research, students who take computer education classes in high school are eight times more likely to major in computers, despite a sharp decline in computer education course enrolment at the high school level over the past 20 years [11]. Pedagogy for a few cybersecurity education programs has been established using mobile and Tablet platforms. Android security labware, for example, focuses on the security of the mobile network, communication, apps, and device along with privacy [12]. Similarly, [13] emphasizes educating users about mobile threats, [14] highlights threats related to mobile web views, and [15] concentrates on mobile malware and security policies.

The technique was used in [16] as a lecture-based technique. A survey was conducted on cybersecurity challenges that impact the knowledge presented in the respective courses. Once the teacher had allotted enough time, she gave the pupils who had chosen to attend a 75-minute lecture. The same subjects were covered as the instructor had previously indicated. An evaluation survey was given to the students after the class. The findings revealed that most thought the cybersecurity themes covered during the lecture were engaging, practical, and relevant.

Malware comes in numerous forms and uses various techniques to spread and infect its victims. Numerous studies have been conducted on security awareness and education, and more are being undertaken. According to a survey by Walaza et al., young people use mobile devices more frequently. As everything becomes virtual and digital, they are employed for various purposes, including social networking and instant messaging [17]. Despite this, everything must take place in a secure setting. Many academic institutes cover security-related themes. Future software professionals and locals should

understand security, which may be accomplished when these courses are offered in academics. This paper discusses mobile applications to improve high school student's knowledge in this domain. This is done using technology that appeals to young students because they are accustomed to using mobile devices. To increase students' knowledge, security awareness exercises are frequently used [18]. Young people are specified as the target audience of cybersecurity activities in this work. Since they are the users and professionals of the future software businesses, this primarily consists of high school and freshmen university students (a section of students typically fresh out of high school).

III. Research Methodology

The responses of 29 students who participated in a 1-week summer camp at the Purdue University Northwest (Hammond, IN) and The University of Toledo (Toledo, OH) were used for the data analysis. Approximately 20 of them were male while the remaining 9 were female. The summer camp was held every day from 9:00 am to 3:00 pm for 5 days. Surveys were given to the pupils at the start and end of each day of the summer camp except an overall camp survey, which was given to the students at the beginning and the end of the camp. Overall, each student responded to 12 surveys. Each survey given to campers was customized to the topics addressed in the lectures and hands-on activities of that day. This survey design method can be an effective technique for learning more about the experiences and learning outcomes of the students throughout the summer camp.

The research for this study examined how much knowledge they have in the area of cybersecurity and the use of smartphones. Based on the evidence acquired, the pupils are not fully aware of the dangers that result from daily security breaches. The majority of security-related cases that occur involve mobile devices, and many of the victims are young students. Teens may need to be made aware of how an application works internally on a mobile device to give them a more detailed insight into how an attacker can steal information without the user knowing. Therefore, the team focused on structuring the overall content to allow students to understand security fundamentals in addition to developing and exercising caution when using mobile applications. The knowledge of security concepts and internals of an application and its architecture will assist the students in comprehending the potential risks associated with using it. The teaching approach combines two subjects into one element, a topic that is crucial for all high school students to learn.

Along with the applications in App Inventor and Anbox during the application development phase, documentation detailing the step-by-step process for designing the application was also provided. When the students read the documentation, they could create the mobile application in the appropriate setting and learn about the security features built into the program. It begins with App Inventor, where students may create apps without writing any code, igniting their interest in future software development and expanding their application development skills. In addition, lecture materials and additional hands-on activities were provided to students to enable learning more comprehensively. Student responses were collected through online Qualtrics-based forms before and after the daily exercises. More details on the surveys and the questions are presented along with the results in Section V. It was also expected that young students might get motivated to pursue a professional career in cybersecurity or mobile app development. The presented work extends on our previous work that introduced some of the apps when they were initially developed [19].

IV. Smartphone based modules

A. Developed Apps

We created five separate online psychological exercises that mimicked real mobile apps that are frequently used. These exercises were developed to educate people about cyber threats and how to avoid them. A "Fake Shopping Application" was utilized in the first activity to show how ransomware operates. The second exercise was a "Fake Quiz App" meant to instruct the participants in cyber-safe practices. The third activity involved using a "Social Media App" to show various social engineering techniques like phishing while simulating a social media platform. A "Chatting App" was used as the fourth activity to inform the participants about the risks of phishing. The fifth and final activity used a "Phony Scareware App" to show how scareware applications function. These apps were created using Android Studio and emphasized the behavior of malware and associated privacy issues. Each of these applications was showcased using an open-source emulator called Anbox.

1) Ransomware App: This application replicates the actions of ransomware, which encrypts all the data in a device when infected and demands a ransom payment to give the cryptographic key used for the encryption. Ransomware is a type of malware that is constantly evolving and is used to encrypt files on a device, rendering them and the systems that depend on them useless. Once the data on the device is encrypted, malicious actors demand a ransom to provide a "key" to decrypt the encrypted files. Attackers using ransomware frequently target their victims and threaten to sell or reveal stolen data or authentication details if the ransom is not paid.

This phony online shopping app was created and set up using Anbox. The user can log in or make a new account from the home page. After logging in, a cart with things already placed in the cart opens. When the user clicks anywhere on the cart, they are taken to a page that requests their payment information after claiming to have encrypted the device, as shown in the figure 1. Using an app that resembles a benign app, students experience a ransomware attack scenario when they use this particular app.

2) Cyber-Safe Techniques: Apps that want access to specific device features without the need for it, such as a game asking for access to the camera or a photo editing app asking for the permission to send and read text messages, are said to

Fig. 1. Fake shopping application (Note: Only for educational purposes, no copyright infringement intended)

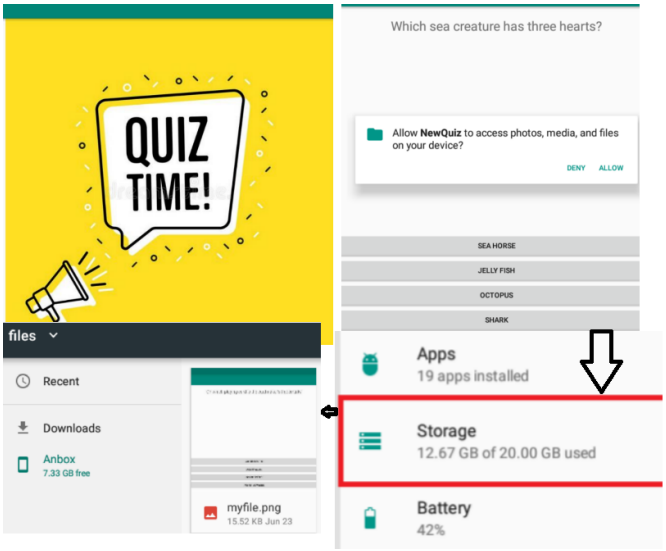


Fig. 2. Fake Quiz App capturing the screenshots while the user is playing the game because of granting irrelevant permissions to the app.

have requested irrelevant permissions. This app replicated this malicious functionality of apps. Granting such permissions to unreliable third-party apps could be harmful as it may allow these apps to steal private information. The developed Quiz app is used to demonstrate this behavior of malicious apps requesting irrelevant permissions.

After launching the quiz app from the Anbox application manager, the user can click anywhere on the screen to begin the quiz. As soon as the user starts providing answers to the questions, the app begins to request unnecessary permissions, such as granting access to files, media, and storage, as shown in figure 2. If the user gives access, one can observe the application saving the quizzes due to granting unnecessary permission. The main objective of this app is to inform students about the importance of adhering to appropriate cyber-safety practices, which includes denying specific access to information that is not relevant to their needs. If such an app is installed on the phone, and it gains access to read text messages, it can potentially read OTPs and other private text messages without user knowledge and send them to an outside email. This functionality could not be demonstrated in the Anbox emulator, so we recorded a video of this example and provided it to students. The video is located at https://www.youtube.com/watch?v=z5DHZypZ-Uo.

3) Phishing: Attacks referred to as "phishing" include sending fake messages that seem to be from a reliable source. Most often, email is used for this. On a smartphone, apps can phish for private login info as well. The intention is to either install malware on the victim's computer or steal personal information like credit card or login information to sensitive applications such as banking. Two applications, that pretend to be popular social media apps, were developed to launch a phishing attack on unsuspecting users. The applications listed below impersonate the real ones while acquiring the user login details. These apps were created with the goal of educating users on how easy it is to become a victim of a phishing attack using popular social media and chat apps.

a) Social Media App: This fake social media application asks the user for their login information and then records it without the user's knowledge, as shown in figure 3. Phishing is a straightforward cyberattack that can target anyone. Therefore, one should exercise caution when providing login credentials to apps or sites accessed through unreliable emails or text messages that do not seem familiar.

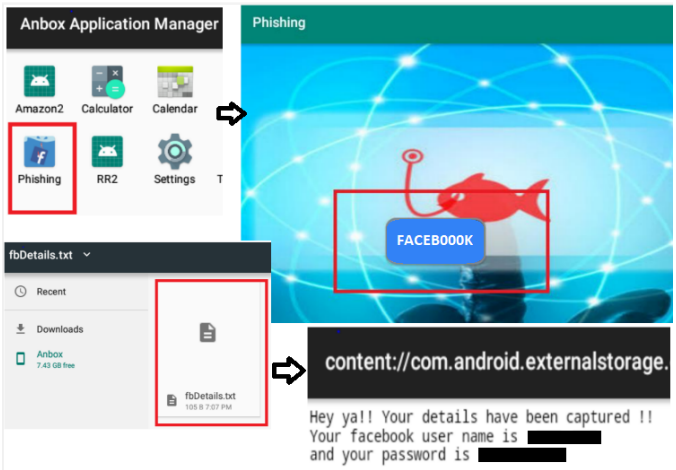


Fig. 3. Fake social media app showing password capture and storage by the app (Note: Only for educational purposes, no copyright infringement intended)

b) Chatting App: This fake chatting app asks the user for their shopping app login information by delivering a counterfeit $500 gift card from an unidentified number to

make it appear authentic. The software tries to save the user's shopping app login information when they log in, as shown in figure 4. This is a different type of phishing scam to show that messages from unknown senders should never be clicked and that no one should ever click on links provided to social networking applications from unknown senders.

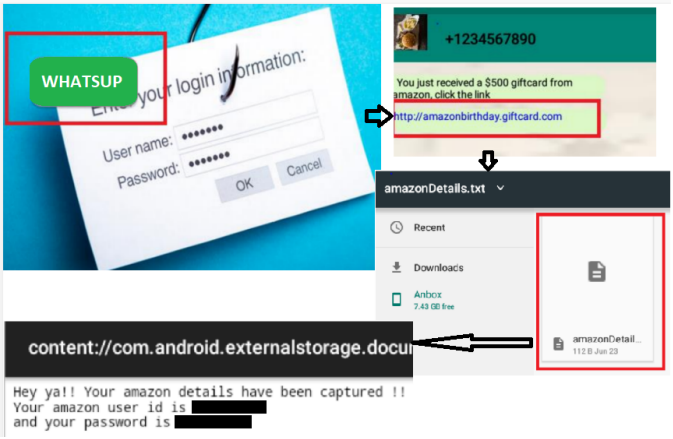


Fig. 4. Fake chatting app showing password capture and storage by the app (Note: Only for educational purposes, no copyright infringement intended)

4) The Scareware App: A malware technique known as scareware deceives consumers into thinking they must download or purchase harmful, occasionally pointless software. Scareware's objectives range from selling pointless, phony utilities to installing dangerous malware that exposes private information. It is among the most dangerous malware because of the novelty of cybercrime and daily increases in financial losses. Understanding the behavior and symptoms of this malware and being prepared will help students defend against it.

This is a false malware app that has been constructed; when users click on one of the bogus notifications, they are taken to a specific page with a button labeled as "Updater." The download progress is displayed via a progress bar if the user presses that button, as shown in figure 5. If no further action is taken, the screen is moved to a warning message, a false alarm meant to cause panic, as shown in the figure 6.

B. App Development using MIT App Inventor

MIT App Inventor, developed initially to teach app development from scratch, can be used to create fully functional apps for Android phones, iPhones, and Tablets. The MIT App Inventor was used to create the following three applications, which were executed in the same Android emulator, Anbox. These examples were afterward used to teach kids about cybersecurity implications in app development. A simple adb install command, shown below, was used to install the developed app's apk file so it could be executed in the emulator.

MIT App Inventor is used to create fully functional apps for Android phones, iPhones, and Android/iOS Tablets, and it's an easy-to-use visual programming environment that even youngsters can use. MIT App Inventor beginners may launch

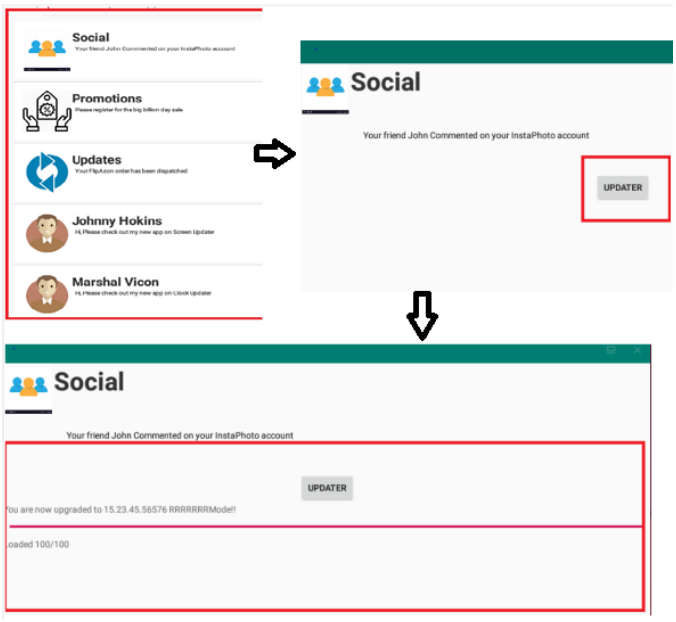


Fig. 5. Phony scareware App attempting to trick user into updating software by sending emails

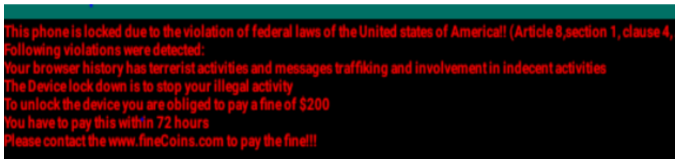


Fig. 6. Warning message from Scareware App when a user updates the software, this message is a false alarm and tries to generate panic to the user.

their first basic app in less than 30 minutes. Programs that teach coding with blocks foster empowerment of the mind and the imagination. Beyond this, MIT App Inventor offers youngsters the opportunity to impact their communities by providing them with the tools needed for building an application using blocks. The app can be installed in Anbox using the following command after it has been created and downloaded as an apk file.

```
$adb install filename.apk
```

The Anbox Application Manager is used to launch the application after installation.

1) The Tiny Banking App
2) The Tic-Tac-Toe App
3) The To-Do List App

a) Installation Process: By using the block programming technique of MIT App Inventor, significant and complex applications were made in lesser time than in standard programming environments. Once the apps are designed, they are compiled, and after successful compilation, the apk file is downloaded as shown in figure 7. Anbox Application Manager displays the app after installing the downloaded apk (Android execuTable) file in the terminal, as shown in the figure 8.

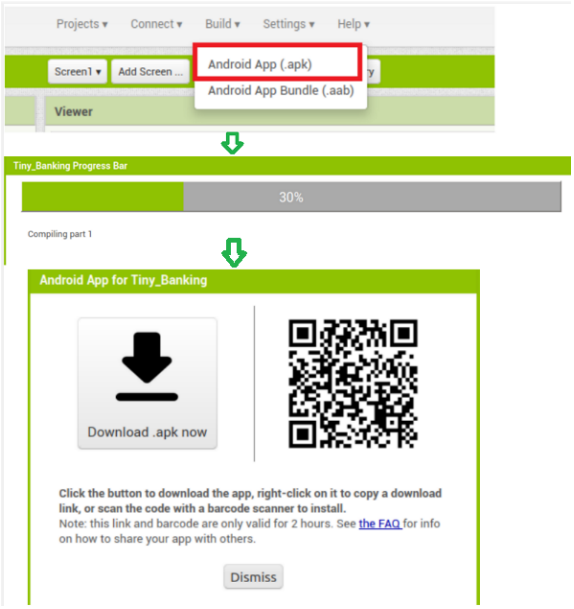


Fig. 7. Figure demonstrating the download of the apk file for the app created with MIT App Inventor after successful compilation.

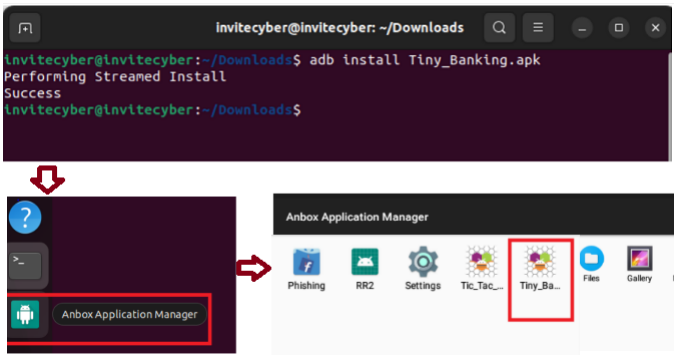


Fig. 8. Figure illustrating how to install the downloaded apk file in Anbox Application Manager.

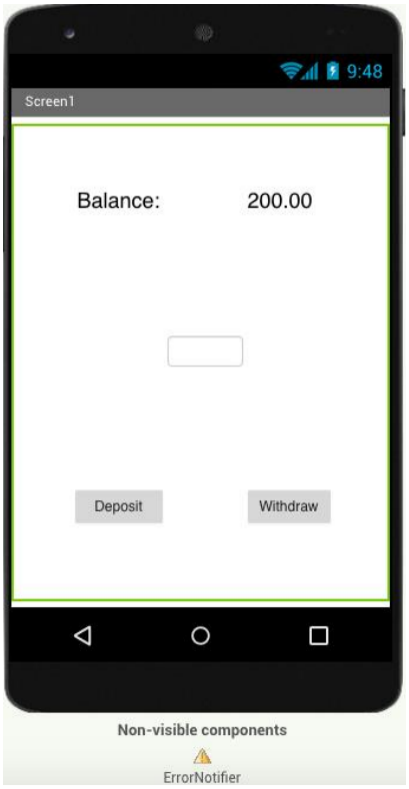


Fig. 9. MIT App Inventor was used to create this Tiny Banking App Application, which has a default balance of 200 and the ability to deposit and withdraw money from the balance.

1) The Tiny Banking App: Nowadays, most big banks offer free smartphone apps that can be downloaded to access their services wherever you are, at least in the United States. Accessing a personal bank account via a smartphone app is powerful, but it also raises many security issues. This application lets users deposit money into and withdraw it from a fake bank account. As an additional security measure, it also checks for specific wrong inputs as a security feature and shows the relevant error message.

Considerations for designing the App:

- To prevent the bank account balance from being altered by adding words, the input text box should be set to "numbers only."
- Since it makes no logical sense to deposit a negative sum of money into a bank account, we should look for deposits that are less than or equal to zero. However, from a security standpoint, allowing users to enter incorrect data into any system, including software, is risky. In this case, letting wrong inputs go undetected could result in stolen bank money.
- The handler for the withdraw button will resemble the one for the deposit button, but it will have an additional condition to check. The majority of American ATMs only allow withdrawals in multiples of $20, and this is due to the ATM only having $20 bills in it. Additionally, we want users to refrain from withdrawing negative sums of money since doing so would effectively add to their account balance by deducting a negative sum. This flaw might be used by an unintentional (or morbidly curious) user to add money to their account.

2) The Tic-Tac-Toe App: Everyone has played tic tac toe a million times throughout their lives. Two players fill in the squares in a 3 X 3 grid of the popular board game tic-tac-toe with either an "X" or an "O" to win. The game is so simple that it shouldn't be too difficult to create an app that mimics it as shown in figure 10. This app can be picked as the first to start with for a better result if the documentation is provided. However, beginner-friendly documents explain the fundamentals of Anbox and App Inventor and provide examples of simple and starter projects for students. The user can begin playing by clicking on any of the 9 available grids, and a reset button makes it possible to restart the game, as shown in figure 10.

Considerations for updating the App: We define known

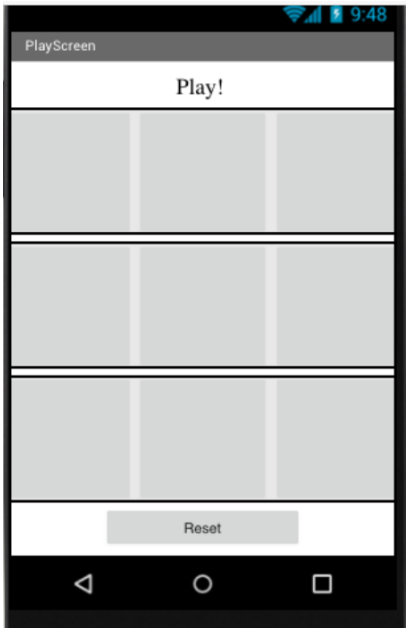


Fig. 10. Tic-Tac-Toe application developed using the MIT App Inventor.

issues for the students so that they may think about the necessity of these issues and whether to fix them.

- The game does not announce whose turn it is at the start of the game, even though it should always be X's turn at the start.
- It is possible to change the font colors of the "X" and "O" to red and blue, respectively, however it is debaTable if this is essential.

3) The To-Do List App: Using MIT App Inventor, we constructed a simplistic, one-dimensional, user-configurable to-do list. The to-do list app will use a "TinyDB" database, unlike the other applications we have created so far, to save any modifications to the list and recall them even if the app has been closed/terminated. This program has only one interactive screen, and the prototype has ten places for to-do task entries. Users may want to use fewer than ten items because each has a corresponding piece of code, and we will put code into the blocks editor for each to-do job we add to the screen. The users can enter a list of tasks that must be completed, and they can be modified at any moment during the day.

The application must update the labels each time the user clicks the "Set" button and store the modifications to the TinyDB. We will require a chain if-else block to provide each list member with this functionality. Although there are only two primary code blocks in our to-do list app, the idea of a database is crucial for application development. Although TinyDB is straightforward, databases as a concept allow for the structured storage of enormous amounts of data. Therefore, this app also aims to educate students about databases.

V. Results

The summer camp attendees at both institutions attempted various quizzes and surveys during the 1-week summer camp

Fig. 11. The to-do list application developed using the MIT App Inventor.

in a pre/post setting. As an outcome of the research, the students, initially unaware of the mobile application development and security concepts, showed a significant improvement in awareness of the app and smartphone security. The documentation of the apps in both the environments, App Inventor and Anbox Application Manager, have laid a foundation for the students to pursue the next steps in terms of their interests. The proper structure of the documentation with the order of preference, starting from beginner apps to higher levels, has motivated them to develop apps much more efficiently. After working on app development and security essentials, the students have shown great interest in further development activities, as they can choose it as a career path either as security professionals or mobile app developers.

A. Web Security

The web security session included the following topics: Why Web Security, Elements of the Web, Introduction to the World Wide Web (WWW), malicious URLs, XSS attack, and SQL injection attack. There were five different ways to respond to the web security surveys: "strongly agree," "agree," "neutral," "disagree," and "strongly disagree". We required a mechanism to transform these category response options into numerical values that could be more quickly and easily statistically assessed to analyze the data gathered from these surveys. One popular method is giving each response option a numerical value on a scale, with higher values denoting stronger degrees of agreement or disagreement using Table I.

TABLE I
MAPPING THE CATEGORICAL VALUES TO THE NUMERICAL VALUES

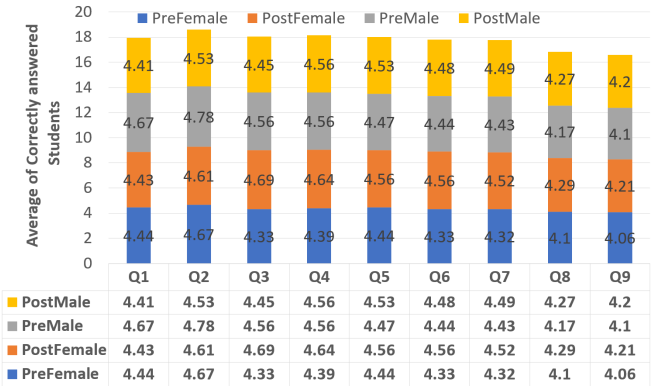
"Strongly Agree": Correct	**"Strongly Disagree"**: Correct
Strongly Disagree : 1	Strongly Disagree : 5
Disagree : 2	Disagree : 4
Neutral : 3	Neutral : 3
Agree : 4	Agree : 2
Strongly Agree : 5	Strongly Agree : 1

For example, take the response "strongly disagree" to the question "Every text you get on your phone originates from someone you know" from the web security survey, which was given a numerical value of 5. We required a mechanism to transform these category response options into numerical values that could be more quickly and easily statistically assessed to analyze the data gathered from these surveys. One popular method is giving each response option a numerical value on a scale, with higher values denoting stronger degrees of agreement or disagreement.

For example, take the response "strongly disagree" to the question "Every text you get on your phone originates from someone you know" from the web security survey, which was given a numerical value of 5. This shows that the statement was highly opposed by participants, who believed it false or wrong. Similar to this, "disagree" received a score of 4, "neutral" received a score of 3, "agree" received a score of 2, and "strongly agree" received a score of 1. We were able to quantify participant responses and create statistical summaries of the data by giving these numbers to each response option. These numbers could be used to determine the average answer for each question for each participant group. In this instance, we were curious to compare how male and female participants responded to the pre-and post-surveys. So, we calculated the mean score independently for each of the four groups—pre-male, pre-female, post-male, and post-female. The average degree of agreement or disagreement with each question among these categories is represented by these means. The pre-and post-surveys results are then separated based on the gender for each question. The questions from the pre-and post-surveys for web security are listed in Table II.

- Pre-Survey Male: consists of the mean of the responses from Male Students to each question in the Pre-Survey.
- Pre-Survey Female: provides the average of the responses from female students to each question in the pre-survey.
- Post-Survey Male: Male student averages from the post-survey are included in Post-Survey Male.
- Post-Survey Female: presents the mean of the responses from female students for each question in the post-survey.

In the figure 12, the averages of the post-survey responses are typically higher or equal to the averages of the pre-survey answers for both males and females. For 6 of the nine items, the means of the post-survey replies for males are more elevated or equal to the averages of the pre-survey responses. For 7 out of the nine items, the standards of the post-survey answers for females are higher than those of



	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
PostMale	4.41	4.53	4.45	4.56	4.53	4.48	4.49	4.27	4.2
PreMale	4.67	4.78	4.56	4.56	4.47	4.44	4.43	4.17	4.1
PostFemale	4.43	4.61	4.69	4.64	4.56	4.56	4.52	4.29	4.21
PreFemale	4.44	4.67	4.33	4.39	4.44	4.33	4.32	4.1	4.06

Fig. 12. Pre/Post comparison for the web app security quiz, by gender.

TABLE II
WEB SECURITY SURVEY QUESTIONS

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 email from an unknown sender is not unsafe.
Q4	Unsafe and insecure URLs do not exist. For example, http://amazonsurprises.com/ and https://amazonsurprises.com/ are same.
Q5	Almost all applications need access to location and Internet services, and there is no harm in allowing these permissions on my 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 it's 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.

the pre-survey responses. This shows that both the male and female participants learned something from the web security summer camp. The participants could retain and apply the knowledge they learned throughout the week, as evidenced by averages that the post-survey responses are typically higher than the pre-survey answers. Females may have had a more excellent grasp or interest in the issues taught in the camp, as seen by the finding that they had higher means for more questions than males.

B. General Cybersecurity

A cybersecurity session on the first day of camp included a variety of topics, including the concept of cybersecurity, the importance of cybersecurity, a discussion of a few recent and past cyberattacks, the CIA triad and threats, vulnerability, attack, and cybersecurity domains. Pre- and post-session surveys were carried out to assess the high school pupils' level of knowledge. Table III shows the survey questions. This survey differed from all others in that there was only one correct answer for each multiple-choice question in the poll, unlike the Likert scale used for other surveys. The correct response receives a 1, while the incorrect response receives a 0.

The average scores for each question for pre- and post-surveys are then determined and displayed on a chart. figure 13 shows that the pre-average survey's score is greater than the post-average survey's score for 2 of the nine questions.

TABLE III
GENERAL CYBERSECURITY SURVEY QUESTIONS

Q1	Cyberattacks harm data and software, but not hardware and physical systems such as power stations, gas pipelines, drones. (T/F)
Q2	In cybersecurity, CIA triad stands for:
Q3	Which of the following does not compromise confidentiality of data?
Q4	Which of the following is violation of integrity?
Q5	If you are not able access your Facebook account, which of the following security characteristics is compromised?
Q6	Which of the following terms refers to weakness in a system?
Q7	A ransomware that scrambles/encrypts your data will not be categorized as:
Q8	Which of the following is most popular smartphone OS?
Q9	Which of the following Android app development software is based on block coding?

This suggests that during the lab sessions and cybersecurity lectures, the students were able to deepen their comprehension of the fundamentals of cybersecurity. Most of the questions had higher average scores in the post-survey than in the pre-survey, indicating that the students had improved their grasp of cybersecurity principles and techniques as a result of attending the cybersecurity summer camp. The improvement in the students' average scores shows that they benefited from the lectures and lab sessions and were able to put their newfound knowledge and abilities to use.

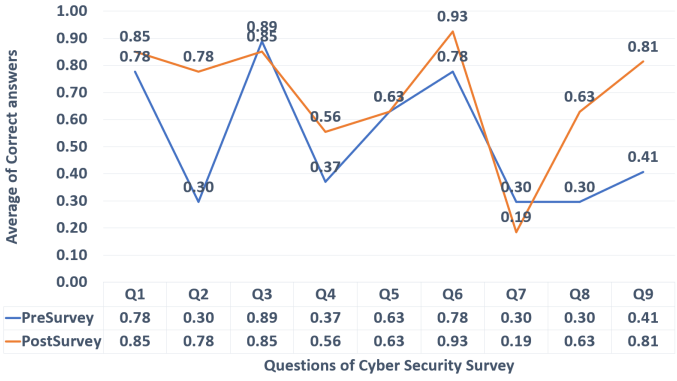


Fig. 13. Pre and Post comparison for general cybersecurity

C. Internet Security

Introduction, categories of Internet attacks, TCP and DNS attacks, and defense technologies are some topics covered by the Internet security session. Table IV lists the questions for the Internet Security Survey. Similar to the Cyber Security session analysis, the pre-and post-surveys of Internet security analysis are shown in the figure 14. It is clear from the post-survey responses from the students that the Internet security-related content successfully raised student awareness of Internet security. Almost all of the questions were correctly answered by the students, and there was a significant improvement in student knowledge after the content was delivered.

D. Cybersecurity as a Career?

The results of the high school students' pre- and post-surveys on cybersecurity as a career are fascinating as shown in figure 15. The findings indicate a shift in the proportion of

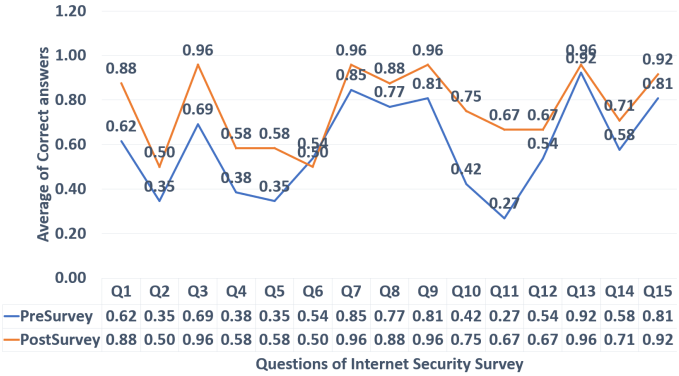


Fig. 14. Pre and Post Surveys comparison of Internet security quizzes.

TABLE IV
INTERNET SECURITY SURVEY QUESTIONS

Q1	Which of the following is most appropriate for Internet?
Q2	TCP/IP is ____ ?.
Q3	Which of the following is an IPv4 address?
Q4	DNS is used to convert ____ to ____ ?.
Q5	Which of the following changes when your smartphone disconnects from your home network and connects with the school network?
Q6	Can a machine have more than one IP addresses?
Q7	Internet has always been robust, safe, and secure from the early days.
Q8	Which of the following is not an attack?
Q9	In IP spoofing, the sender uses a fake IP address for the source address instead of its actual address.
Q10	A TCP connection between client-server is set up through a handshake.
Q11	Which of the following causes Denial-of-Service?
Q12	In DNS cache poisoning, attacker tricks the local DNS server or system to store an incorrect ____ for a hostname.
Q13	We should use a website that uses HTTPS.
Q14	VPN sends our traffic through an encrypted tunnel in untrusted network.
Q15	We should prefer to use a VPN in public Wi-Fi.

students who wish to pursue cybersecurity as a career. 30% of the students who responded to the pre-survey somewhat agreed, 18% somewhat disagreed, and 11% strongly disagreed that they should pursue cybersecurity as a career. However, the proportion of students who partially agreed rose to 55% in the follow-up study. This significant increase shows that there is a more substantial interest in the subject as a result of the lectures and practical activities. The proportion of students who somewhat disagreed, on the other hand, has dropped from 18% to 10%. After the lectures, fewer students were hesitant or doubtful about pursuing a career in cybersecurity. The proportion of undecided students has likewise dropped from 19% to 14%. This can be interpreted as a sign that students have increased confidence in their career decisions due to learning about cybersecurity. It's crucial to remember that the proportion of students who strongly disagreed also rose from 11% to 14%. This demonstrates that there is still some reluctance to choose cybersecurity as a career, and more efforts may be needed to raise awareness and motivate students in this direction.

VI. CONCLUSION

Malware attacks and cellphones are currently in the spotlight due to recent advancements in mobile technology. Similar

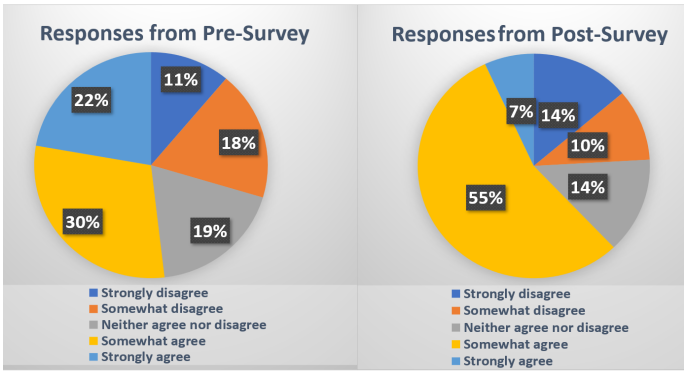


Fig. 15. Pre and Post Surveys comparison for the survey question "I am interested in pursuing cybersecurity as a career?".

to the assaults targeted at PCs, Drift reveals a dramatic increase in mobile malware. Regarding user and mobile device awareness of information security, there were two main settings in which mobile applications were built. The primary subject of the paper is the creation of applications that teach students how to create apps while simultaneously paying attention to security. With the help of these apps, an effort was made to conduct psychological training for high school students to identify cybersecurity threats, preventing them from falling victim to a cyberattack and boosting their confidence to pursue cybersecurity as a career. One strategy for addressing the requirement for security awareness is to include mobile device security in the curriculum.

The apps could be improved in the future to make them more user-friendly and "realistic," and allow integration of additional capabilities and deeply addressed security issues. Contents ought to be updated because security risks evolve over time. When creating mobile applications, gaming elements can also be introduced. Students now have a better understanding of these problems and are better equipped to handle them in their future careers as professionals. The globe is advancing toward a more modern state as the economy expands. Malware and cyberattacks will also grow at the same rate, but there aren't enough cybersecurity experts around the globe. As students gain knowledge in the area of cybersecurity, this strategy will help grow the workforce. According to the findings of the surveys, pupils' learning was improved.

VII. Acknowledgement

This material is based upon work supported by the National Science Foundation under Grant Nos. 1903419 and 1903423 through the Security and Trustworthy Cyberspace Education (SaTC: EDU) program. Any opinions, findings, 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 as an Exempt Study by the Institutional Review Boards at Purdue University Northwest (Hammond, IN) and The University of Toledo (Toledo, OH) under protocol numbers IRB-2020-1119 and IRB-301407-UT, respectively.

References

[1] A. Achten, "Identity Theft Resource Center Q3 2022 Data Breach Report: Compromises Victims Up from Q2 – Record High Year Unlikely." https://www.idtheftcenter.org/post/q3-2022-data-breach-report-compromises-victims-up-record-high-year-unlikely/, 10 2022. Accessed Nov 20, 2022.

[2] R. Vogel, "Closing the cybersecurity skills gap," *Salus Journal*, vol. 4, no. 2, pp. 32–46, 2016.

[3] L. Drevin, A. Le Grange, and M. Park, "The concept of mobile applications as educational tool to enhance information security awareness," *de SACLA, Magaliesburg, South Africa*, 2017.

[4] A. Holzer and J. Ondrus, "Trends in mobile application development," in *Mobile Wireless Middleware, Operating Systems, and Applications - Workshops* (C. Hesselman and C. Giannelli, eds.), (Berlin, Heidelberg), pp. 55–64, Springer Berlin Heidelberg, 2009.

[5] A. A. Adekoya, A. M. Donald, S. Akkaladevl, and A. A. Akinola, "Empirical evidence for a descriptive model of principles of information security course," *Journal of Information Security*, vol. 11, no. 4, 2020.

[6] B. L. Clouse, *An Explanatory Sequential Mixed Methods Study: Examining the Effects of an Onboarding Training Program on Organizational Socialization and Commitment in a Middle Eastern Energy Company*. Drexel University, 2020.

[7] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973–993, 2014.

[8] N. Malviya, "Computing degree and enrollment trends." https://resources.infosecinstitute.com/topic/9-best-practices-for-network-security/. Accessed Nov 20, 2022.

[9] S. Mansfield-Devine, "Android malware and mitigations," *Network Security*, vol. 2012, no. 11, pp. 12–20, 2012.

[10] G. Jin, M. Tu, T. Kim, J. Heffron, and J. White, "Evaluation of game-based learning in cybersecurity education for high school students," *Journal of Education and Learning*, vol. 12, pp. 150–158, 2018.

[11] S. Zweben, "Computing degree and enrollment trends." http://archive2.cra.org/uploads/documents/resources/taulbee/CRA_Taulbee_CS_Degrees_and_Enrollment_2012-13.pdf. Accessed Nov 20, 2022.

[12] M. Guo, P. Bhattacharya, M. Yang, K. Qian, and L. Yang, "Learning mobile security with android security labware," SIGCSE '13, (New York, NY, USA), p. 675–680, Association for Computing Machinery, 2013.

[13] A. S. Peruma, S. A. Malachowsky, and D. E. Krutz, "Providing an experiential cybersecurity learning experience through mobile security labs," *2018 IEEE/ACM 1st International Workshop on Security Awareness from Design to Deployment (SEAD)*, pp. 51–54, 2018.

[14] W. You, K. Qian, D. C.-T. Lo, P. Bhattacharya, W. Chen, T. Rogers, J.-C. Chern, and J. Yao, "Promoting mobile computing and security learning using mobile devices," in *2015 IEEE Integrated STEM Education Conference*, pp. 205–209, 2015.

[15] X. Yuan, K. Williams, S. McCrickard, C. Hardnett, L. H. Lineberry, K. Bryant, J. Xu, A. Esterline, A. Liu, S. Mohanarajah, and R. Rutledge, "Teaching mobile computing and mobile security," in *2016 IEEE Frontiers in Education Conference (FIE)*, pp. 1–6, 2016.

[16] H. Chi, "Integrate mobile devices into cs security education," in *Proceedings of the 2015 Information Security Curriculum Development Conference*, InfoSec '15, (New York, NY, USA), Association for Computing Machinery, 2015.

[17] A. Sharma, M. C. Murphy, M. Rosso, and D. Grant, "Developing an undergraduate information systems security track," *Information Systems Education Journal*, vol. 11, no. 4, p. 10, 2013.

[18] M. Koyuncu and T. Pusatli, "Security awareness level of smartphone users: An exploratory case study," *Mobile Information Systems*, vol. 2019, 2019.

[19] L. M. Podila, J. P. Bandreddi, J. I. Campos, Q. Niyaz, X. Yang, A. Trekles, C. Czerniak, and A. Y. Javaid, "Practice-oriented smartphone security exercises for developing cybersecurity mindset in high school students," in *2020 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, pp. 303–310, IEEE, 2020.