Practice-Oriented Smartphone Security Exercises for Developing Cybersecurity Mindset in High School Students

Laxmi M. Podila
EECS Department
The University of Toledo
Toledo, OH, United States
lpodila@rockets.utoledo.edu

Jyothi P. Bandreddi
EECS Department
The University of Toledo
Toledo, OH, United States
jbandre@rockets.utoledo.edu

Javier I. Campos
ECE Department
Purdue University Northwest
Hammond, IN, United States
jicampos@pnw.edu

Quamar Niyaz
ECE Department
Purdue University Northwest
Hammond, IN, United States
qniyaz@pnw.edu

Xiaoli Yang
ECE Department
Purdue University Northwest
Hammond, IN, United States
yangx@pnw.edu

Anastasia Trekles
Instructional Design
Centier Bank
Merrillville, IN, United States
atrekles@gmail.com

Charlene Czerniak
College of Engineering
The University of Toledo
Toledo, OH, United States
charlene.czerniak@utoledo.edu

Ahmad Y. Javaid
EECS Department
The University of Toledo
Toledo, OH, United States
ahmad.javaid@utoledo.edu

***Abstract*—Advancements in technology and the increase in Internet usage through mobile devices have led to greater visibility of organizations and individuals to cybercrimes. Teenagers being easy targets of these cybercrimes, there is a need to educate them on cybersecurity trends since training students on existing cyberattacks is viewed as a powerful tool to teach cybersecurity. We present a pedagogical approach to train students to identify new threats and respond to mitigate them. This is accomplished through observatory, experiential, and real-life practice-oriented cybersecurity exercises. Seven malicious android applications targeting malware class and phishing, namely Email-Lite-Scare, Shop-Shock-Struck, Cyber-Safe Practices, Play- Read-Disrupt, Fish-A-Phish, Chat-Phish, and Spy-The-Trojan, have been developed. Psychological learning is emphasized in this approach by exercising the application extensively. The underlying goals of this work are to develop a security mindset, spread awareness on threats associated with smartphone/tablet usage, and to inculcate interest in cybersecurity careers among high school students.**

***Keywords*—cybersecurity education, security mindset, smartphone apps**

I. Introduction

Tremendous technology growth, increased Internet usage, and users' heavy reliance on them pose serious threats to security and privacy in this digital world. In past two decades, we have witnessed many cyberattack incidents targeting individuals, businesses, and government organizations. On an average, an attack was reported to a computer with Internet access worldwide for every 39 seconds in 2019 [1]. The number of data breaches in the US increased by 900% in 2019 compared to 2005 that led to jump in the number of exposed records by 250% in the same time frame. Around 914 million identities were exposed in 2018 [2]. A data breach cost around $3.92 million on average in 2019 and it has been forecasted that worldwide spending on cybersecurity will reach $134 billion in 2022 [3].

The growing rate of cybercrime incidents exceeds the human resources available for defending against them, thus creating a huge cybersecurity skill gap [4]. According to cybercrime magazine, the cybersecurity skill gap will create 3.5 million unfilled jobs in 2021 [5]. At the same time, teenagers are one of the most vulnerable targets of cyberattacks as they may have high-level of trust in people and low-level of cybersecurity knowledge [6]. For instance, they often install game or entertainment apps without knowing their consequences, browsing web on open platforms, befriend people on social networking sites, access Internet through public Wi-Fi without giving any thoughts. Along with the lack cyber-safety practices, they also lack cybersecurity occupational interest [7]. There is a need of standard curriculum for cybersecurity education from school level to strengthen the cyber-safety practices and develop a cybersecurity mindset in the students from an early age [8]. This will also shorten the cybersecurity skill gap by inculcating interest in students to choose cybersecurity as a career [9].

According to "Business of Apps" first quarter report in 2019, 2.6 million Android and 2.2 million iOS apps are available in their respective app stores for 5 billion smartphone users [10]. The users' dependency on smartphone apps for their daily lives' activities lead to increased cybersecurity threats. 56 Android apps designed for children have been discovered as malware that infected 1.7 million devices through fraudulent ads, and links [11]. The school students fail to identify the significant indications of such threats as they are surfaced under benign working features of the apps [4]. Educating students by introducing them to apps that act maliciously will help them identify fraudulent behavior in malware apps. With a psychological approach to identify adversaries, we plan to help high school students by providing a set of mitigation guidelines [12]. With this motivation, we built Android apps targeting malware and phishing categories for cyber-psychology exercises that will develop security mindset, spread awareness on threats associated with the smartphone usage, and inculcate interest for cybersecurity as a career among the high school students.

The remainder of the paper is organized as follows. Section II summarizes the previous efforts for cybersecurity education and draws focus on the novelty of the work presented in this paper. In Section III, we discuss the smartphone apps developed for cyber-psychology exercises. Finally, the paper is concluded with future work direction in Section VI.

II. Related Works

Many cybersecurity education initiatives with innovative pedagogical techniques have been taken in the last few years to bridge the skill gap between future workforce and exponentially increasing demand for cybersecurity professionals. The most explored ways for delivering cybersecurity education include game-based approaches [13], CTF (capture the flag) competitions [14], robotic platforms [15], and hands-on activity based programs [16].

With the advent of online education, the use of smartphones and tablets as content delivery platforms have been skyrocketing. However, offering cybersecurity education by focusing security issues in them is not widely adopted. Also, identifying the knowledge areas and delivering them to the students in an efficient and age-appropriate fashion is a real challenge. We identified the knowledge area 'Malware and Attack Technologies' as our focal point. Our approach, seemingly on par with other smartphone based approaches, begs to differ in the impact area and methodology. Concentrating on state-of-art malware apps considered by a few to none cybersecurity bootcamps makes our research first of its kind. The cyber-psychological exercises offered through our malicious apps have two primary goals: (1) develop a cybersecurity mindset to identify threats and mitigate them by understanding the adversary's objective, (2) help students to use their observatory skill and become proactive and vigilant.

A few cybersecurity educational programs have developed pedagogy through mobile/tablet platforms. Android Security Labware concentrates on device security and privacy, app security, mobile network, and communication security [17]; [18] focuses on educating threats launched via mobile, [19] emphasizes on the threats associated with web view mobile; [20] and [21] focus on mobile malware and security policies. A few educational programs teach cybersecurity through secure software development by utilizing mobile app development and reverse engineering of apps [22], [23]. A few programs focus on mobile databases and NoSQL database security with Android-based hands-on activities and role-based security labware [24]–[26]. Other portable and pocket lab applications for cybersecurity education released on play store are [27], [28] and [29]. [30] is released as an anti-virus educational mobile security enhancement application. Lastly, programs such as [31] and [32] are designed to include the hands-on activities in already existing cybersecurity, computer science, mobile security and/or network security courses.

III. Smartphone Apps for Cyber-psychology Exercises

We discuss seven apps developed for cyber-psychology exercises. These apps are developed in Android platform and focus on highlighting the malware behavior and privacy distortion. Each app is discussed in the following format:

- **Attack:** The type of threat associated with the app.
- **Objective:** The purpose of the app and the need for study.
- **Design:** Discussion on the design and user interface of the app.
- **Functionality:** User's perspective on app's flow.
- **Explanation:** Attacker's perspective on the screening of the attack in the app.
- **Impact Area:** App's focus on students' psychological, analytical, and emotional behaviors. The skills and areas of impact have been focused.

A. Email-Lite-Scare: Delivering Scareware through Small Fake Apps

Attack: Scareware is a malware that uses social engineering to create shock, anxiety, and fear. With the illusion of a threat, it forces the victim to buy or install unwanted software.
Objective: The novelty of cybercrime and increased financial losses each day make scareware one of the most threatening malware. To defend against this malware, knowledge of its behavior and symptoms and preparedness are beneficial.
Design: Email-Lite-Scare, as the name suggests, is an email system impersonating lite version of an email delivery app.
Functionality: From end users' perspective, the app opens a list of emails resembling the classic email systems' mobile version. The elements in the list are *Social*, *Promotions*, *Updates*, and personal email messages with the subject *"Please look at my new screen updater"*. Each email opens into a new screen with an email label, email subject, and an empty email body with a button named *Updater*. On the button click, a progress bar is populated. When the progress meter shows 100%, an acknowledgment is displayed above the progress bar stating that the device has been updated to *15.23.45.56576 RRRRRRRMode*. As soon as the acknowledgment appears, it is navigated to a screen with a warning text, as shown in Fig. 1.

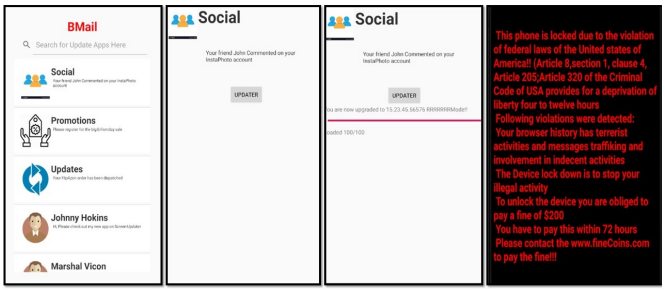

Fig. 1. Scareware Demo Application

Explanation: A set of email look-a-like list, is presented to the user without any authentication. All the emails contain the same *Updater* button in the message area. Safe online practices report provides statistics that the button will be clicked by at least 70% users. The provided progress bar and acknowledgment will project to have downloaded and updated to a fraud 15.23.45.56576 RRRRRRRMode. After a few seconds, a screen with a scary message written in red, bold letters is shown on the user's mobile device. The user is free to open and close the app; the message creates fear, triggers danger and confusion that lead to doubts on the security of the device even when the device works perfectly fine.
Impact Area: Scareware targets human emotional and psychological behavior. With such warning messages, people may buy online false anti-virus schemes claiming to give immediate and all-around protection. Even after a complete virus check, these apps cause mental stress to the user. Complex attacks via such malware may cause public havoc and lead to serious issues.

B. Shop-Shock-Struck: Pretend Ransomware and Panic Creator

Attack: Ransomware is a malware that trades to unlock a device or decrypt user's files on the device that were held for a ransom.

Objective: We aim to familiarize students with the tricks and pranks of ransomware.

Design: Shop-Shock-Struck follows the leading online shopping app's model. It has home screen to choose options, sign-up page, login page, shopping cart page, and payment site.

Functionality: The app opens with the home page where a user is asked to login or create a new account. To ensure this process, two buttons direct to their respective login and sign-up pages, along with a link "*Need Help?*". If the login button was clicked, the control is transferred to the login page to access the shopping account. When the submit button is clicked, the screen shifts to a pre-loaded cart amounting to $8998.96 shown in Fig. 2. A tap on the screen takes the user to a page with a scary skull, warning message, and a *Proceed to Pay* button. Once the user updates the page with all the required details and clicks the button *Pay Ransom*, the page navigates to a black screen with a link and a scary message. The navigation options in the app such as *Back*, *Home* and *Overview/Recent apps* are blocked.

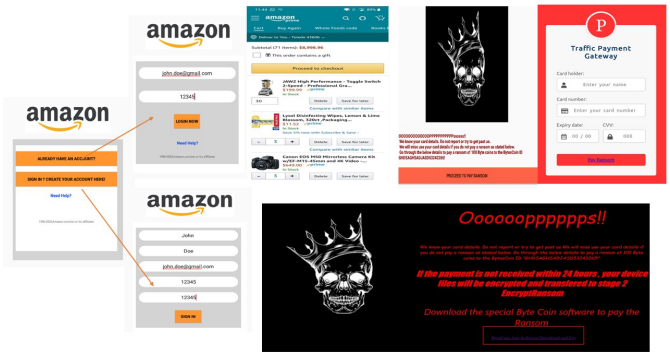

Fig. 2. Ransomware Demo application

Explanation: A stacked shopping cart image with 71 random things, adding up to $8998.96, is the end result of all the authentication ways. After a single click on the shopping cart image, the control is moved to a page where the main *"shock"* occurs. A scary admonition message with a *"Proceed to Pay"* button is present. The user may attempt to return to the previous screen or exit the application, at this point the *"Struck"* activity is featured to the user. The back and overview buttons both return to the current screen. When the home button is clicked, after 30 seconds, the app reopens itself. If the user picks the alternative *"Proceed to Pay"*, a fake payment site in a Webview is opened that takes credit card details. When the *"Pay Ransom"* button is clicked, second *"Shock"* is uncovered. The links on this page switch back and forth between the payment and scare message. On all the screens, the *"struck"* activity holds the equivalent.

Impact Area: With this hands-on activity, our objective is to make students acquainted with ransomware, help them comprehend the preventive conduct, and prepare them tackling ransomware apps. We emphasize on emotional and psychological behavior through this app.

C. Cyber-Safe Practices

Internet access is increasing day by day and the number of digital attacks are growing in the same rate. Therefore, cyber-safety has become a major concern nowadays.

Attack: This section demonstrates two apps, showcasing irrelevant permission requirement and privacy distortion.

Objective: We intend to show students that in any event when there are no indications of eccentric conduct, there could be potential possibilities that the app is malicious. We also promote to use trusted apps/games and understand run-time permissions. The main motive of these apps is to help students understand the importance of cyber-safety practices.

Impact Area: These two apps let the user understand the need and practicing of cyber-safe behavior. The disruptions showcased through the app will be possible only when the user accepts permissions irrelevant to them often leading to theft and privacy concerns. With these apps, we aim to focus on improving students' attentive behavior and observatory skills.

1) Play-Read-Disrupt: Tic-tac-toe– A Privacy Distortion:

Design: A 3x3 tic-tac-toe game has been designed for two players. Two dynamic texts display the players' scores and a reset button to reset the game at any point shown in Fig. 3.

Functionality: A big rectangle divided into nine equally divided grey rectangles are placed in the center of the screen. All the moves that happen at the odd count will be made by the first player and marked as 'X', while the even moves are made by the second player and marked as 'O'. With every move, the system is programmed to compare the symbol with the adjacent and diagonal grids to declare the result of the game. The game supports all forms of results win, lose, or draw. After the game is finished, the scoreboard on the top left is updated and all the boxes are cleared for the next match.

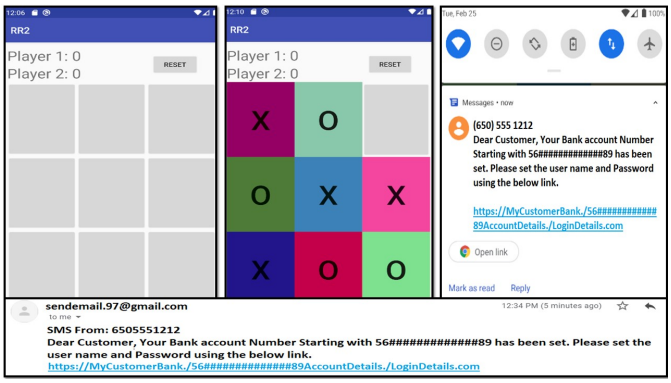

Fig. 3. The tic-tac-toe game

Explanation: Along with intercepting the incoming messages, the app is programmed to email the messages with the sender's information to the attacker shown in Fig. 3. The extensions of this app may range from stealing personal information to other important details stored on the victim's device. If the user opens the app at least once after its installation on the device, the messages on the device until that point are all sent to the attacker through emails, even when the user exits the game just after 30 seconds. The operation of sending emails in the background is triggered by accepting the "read messages" permission requested by the app. If the user is not cyber-aware, he/she will allow the permission and fall into trap.

2) Quiz Your Permissions: **Design:** Cyberattacks can happen through fun and educational activities as well. We presented a run time permission misuse attack in a fun, easy, and interactive quiz app, where users could test their general knowledge. The quiz follows a multiple-choice pattern.

Functionality: The user plays a quiz of 10 questions. As soon as the app is launched, a quiz poster is shown on the homepage that directs the user to a proper quiz with questions along with four choices. This is a general quiz intended for fun and has trivial questions. As soon as the user starts answering the questions, a permission alert pops up asking *"Allow Quiz to access photos, media, and files on your device?"*. This alert is similar to permission alerts in Android apps, and the user has to select an option between *"Deny"* and *"Allow"*. Before continuing the quiz, the user must select one of the options. Afterward, the user may continue playing the quiz until all the questions are answered. When the user chooses a correct answer to a question, the user may go to the next question, while an incorrect response would require either quitting or starting a new session.

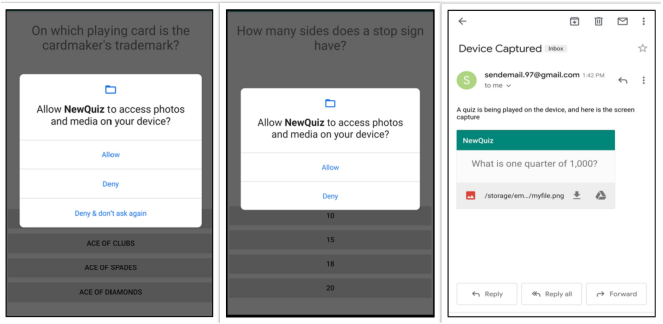

Fig. 4. Quiz Your Permissions

Explanation: This quiz app requests accessing device media, which is not required to play the quiz. If the user opts *"Deny"* to deny the media access, the permission alert repeatedly pops up until (s)he clicks on *"Allow"*. On approval to access the media, a screenshot of the current screen is saved in the phone memory and is sent over an email to a designated attacker for every question answered in the quiz. The user is unaware of this information theft as the email details are embedded in the app. However, they can view the screenshots in the device using the file manager. The user might delete the suspicious screenshots from the device, but the damage has already been incurred when (s)he granted irrelevant permissions. The malicious activity will continue until the user terminates the app. Fig. 4 briefs the app functionality, including the email received at the attacker's end.

D. Fish-A-Phish

Phishing is the most common attack that leads to data breaches. In phishing, the attacker uses deceptive methods to gather sensitive information, such as passwords, credit card, and banking details. These phishing attacks target teenagers, benefiting from their naive understanding of the Internet, and ignorance of cybercrime. These attacks can happen within a few seconds through simple actions such as clicking a link or downloading an app from the Internet. We developed two apps that replicate most common phishing attacks. The idea behind developing these apps is to demonstrate students that their information can be stolen without notice.

1) Social-Phish:

Attack: The effects of downloading mobile apps from non-trusted third-party websites.

Objective: As per CPO magazine, approximately 71% of the attacks on mobile devices happen through apps and browsers. This app presents a scenario to let the user understand the implications of accepting fake app updates.

Design: Social-Phish is developed as a replica of the most popular social networking app, pretending to be the original one.

Functionality: Upon launching this app, a login page asks the user for Facebook credentials. The user must provide the credentials and click "Sign In" to continue. The server continues to buffer and delays loading the home page when an alert pops up with a message. *"There's some connection error. Please login through web page"* The users are redirected to the web login page where they can proceed by providing their credentials.

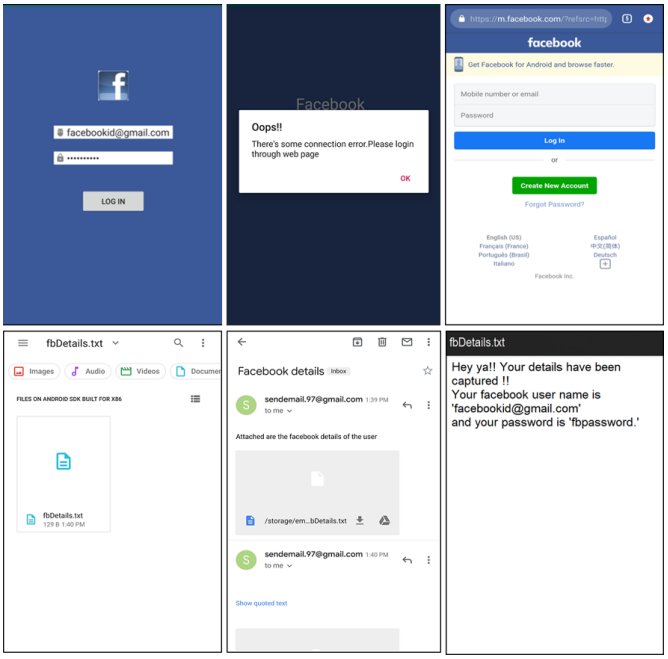

Fig. 5. Functionality of Social-Phish app

Explanation: Once the user enters the required information in the fake Facebook login page, it embeds the login credentials into a text file and saved in the device memory. This happens even if the user terminates the app instead of continuing through browser login. Once the file is saved, it is sent over an email to the attacker. The user can access the text file generated through the file manager, not the email as it is sent in background.

Impact Area: This app helps to understand that a mobile device can be tracked even without user approval. Therefore, the user must update mobile apps only through official/legitimate sources without naive adherence to the app instructions.

2) Chat-Phish:

Attack: This app replicates a scenario of a Phishing attack that may occur when an individual attempts to access unsecured URLs or access a captivating message from an unknown number.

Objective: The intention behind developing this app is to let users know how they can be a victim of a cyberattack, just

with a click. To emphasize on understanding the differences between secured and unsecured links.

Design: The interface of this app is similar to the famous chat app, *Whatsapp*. The familiarity with WhatsApp helps us to include malicious behavior inside a benign chat app. Later, it adapts the interface of Amazon shopping app, where the user's credentials are captured to misuse.

Functionality: When the app is launched, the user encounters a misleading button that directs to a page displaying a list of messages along with a message from unknown number *"You have received a $500 gift card from Amazon as your birthday is sooner. Click on* http://amazonbirthday.giftcard.com *to claim."* When the user clicks the link, an alert pops up saying, *"Please login to Amazon to continue"* and switches to an Amazon login page where the user is requested for authentication. On providing the details and clicking the "Sign In", it prompts an error *"There's some connection error. Please login through the web page."* This alert navigates to the login page of Amazon.com in the browser, and the user can proceed by providing the necessary information for login.

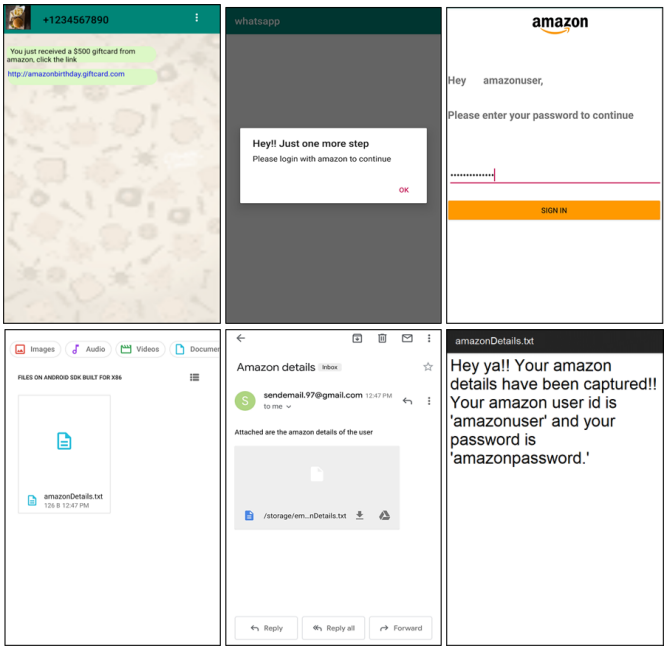

Fig. 6. Functionality of Chat Phish app

Explanation: As soon as the user enters his/her credentials, a text file with the given credential is created in the internal storage device, and this file is sent via email to the attacker. Like the functionality of the social media app, the saved text file can be accessed in the device storage, but not the sent email.

Impact Area: This app demonstrates that any message from an anonymous number cannot be trusted, even when it appears to have some important information, and clicking on unsecured links is often perilous and might lead to identity theft.

E. Spy-The-Trojan: A Musical Instrument App

Attack: Spyware is classified as a type of malware designed to infiltrate and gain access to your device's internet usage data and sensitive information. This malicious app comes in the form of a Trojan horse.

Objective: Spyware can gather data and monitor nearly any activity on a device. Its potential for malevolent use is not limited to files on hard drives but also temporary data such as screenshots and data packets on connected networks. We attempt to provide an understanding of spyware in the form of a Trojan horse. Students are exposed to spyware, Trojan horses, permissions, and basic networking concepts.

Design: The app is a musical instrument and serves as a Trojan horse for spyware. It serves as a musical keyboard for the Piano or Harpsichord. The app consists of two activities, the first being the keyboard itself and accessed immediately after launching. The second is a setting activity where users can customize the keyboard layout, scale, instrument, and color scheme.

Functionality: The app is a musical instrument and serves as a Trojan horse for its nefarious activities. When the app is launched, it asks permission to use the Internet and storage access. When the app is launched, the hexagonal shaped keys are rendered immediately. A toolbar is located at the top and used to switch back and forth between activities. The toolbar has two extra buttons that allow a user to zoom in and out and to scroll through the keys. Fig. 7 shows the two activities and the toolbar used to navigate between them.

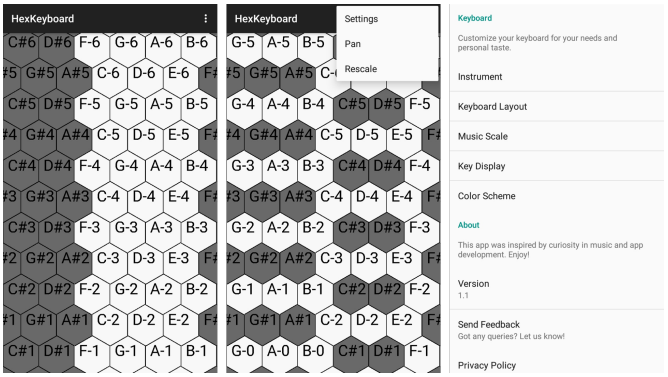

Fig. 7. Screenshots for the music app's main and settings activities.

Explanation: An attacker will receive photos from users who give the app full permission. Whenever a user takes a photo, and the application is open in the background, the attacker will receive a copy of that image. The app does not indicate that the app accessed the smartphone's image gallery or accessed the Internet for that

matter. The app has a hard-coded URL where it forwards a copy of all newly created images. When the malicious app has been installed onto a device, the attacker idly stands by while photos are sent and collected on a personal server hosted by the attacker. We have set up a basic web server to handle incoming images and save them into a directory.

Impact Area: Trojan horses are deceitful, and permissions must be granted only when needed. Spyware preys on users' lack of awareness because they don't realize the vast amount of data accessible to the apps. To counteract this, users should be conscious of their decisions and limit the data available to seemingly benign apps.

IV. Cyber-Psychology Exercises as Teaching Enhancements

Teaching cybersecurity can be a tedious and brain storming, preparing the visually captive clippings and exercises to support the information presented in class. Cybersecurity

study is proved to be effective with hands-on activities. Students should also have a grasp of the real cyber attack in a given situation to analyze and familiarize with cybersecurity. With such requirements at hand, teachers in the cybersecurity field can include hands-on activities, games or conduct CTF challenges in class sessions. While developing the required games and activities from scratch can be time consuming, using already existing open source resources can be very helpful. Activities like role playing, poster making, puzzles and decoding challenges can also be modelled easily on a given cybersecurity topic. We would also encourage teachers to utilize the applications presented in this paper to introduce students to cyber-attacks. Students exercising the application on their own can bring a great deal of enlightenment in themselves compared to the knowledge gained after plain teaching. Using such activities can inculcate interest in students to learn more about cybersecurity issues. As verified in the results section, using the cyber-psychology exercises presented in this paper to teach cybersecurity has been proven to be impactful.

As part of our cyber-psychology exercises, we have developed in-house cybersecurity material including the fundamentals required for cybersecurity education. We have designed 10 PowerPoint presentations. Each of these presentations vary from 20-50 slides with intuitive, graphical and engaging cybersecurity material. The sessions include and are not limited to: Introduction to Cybersecurity, Cryptography, Information Security Assurance, Internet, Malware, Phishing, Principles and Policies, Real world security problems, Secure Cyber Practises and Society and world. The detailed description of the information presented in these sessions is presented in the table I. We plan to design application for each session mentioned in the table I and develop a complete week-long cybersecurity summer camp for high school students. The applications and cybersecurity material can be made available if requested by teachers from other institutions.

TABLE I
A GUIDE FOR TEACHERS

Session	Focus Area	Apps Used
Intro. to Cyber Security	History & importance of Cyber Security, Types of Cyber Attacks, CIA triad, Ethical Hacking, Cyber security careers	–
Cryptography	Types of Cryptography, How & Where to use Cryptography?, Real world examples using Cryptography.	–
Information Security Assurance	Information Assurance model, Aspects, Key role plays, IA Process, Security Paradigm	–
Internet	Web history, development, working & connecting to Internet. General concepts.	–
Malware	Malware, Targets of Malware Recent Malware Attacks, types of Malware, Malware Prevention & detection	Email-Lite-Scare, Shop-Shock-Struc-k, Spy-The-Trojan
Phishing	Phishing Scams; Identify, respond & protect from Phishing emails, Targets of Phishing Scams, Reporting Phishing	Social-Phish, Chat-Phish
Principles & Policies	Principles of Cyber Security, Expert Principles on Cyber Security, Top 6 Security Policies, Policies/Standards of Cyber Security	–
Real World security Problems	Threats launching, Industry losses, Cyber Security & future	–
Secure Cyber Practises	Common mistakes people do, Secure Cyber Practices	Play-Read-Disrupt, Permissions Quiz, Spy-the-trojan
Society & World	Statistics on vulnerable countries & most prepared countries to fight cyber crime.	–

V. EVALUATION AND RESULTS

The applications presented in the section III have been given to freshmen students at the University of Toledo who were taking the "Introduction to Computer Science and Engineering" course in Fall,2020. Considering the COVID-19 pandemic restrictions, we used online open tool APKONLINE to host the android apps and let students explore. To accomplish this at ease we provided end-to-end documentation on how to access each application and what are the key observations to be made. Our goal was to point students in the direction of self-learning, observation and identification. To analyze the impact of these educational android applications, we have designed pre and post surveys inline with each application. Prior to providing the applications, we gave all the pre-surveys as an assignment to the class of 97 students. Later we presented our applications through online tool APKONLINE which was followed by the post surveys. A CLASS-based survey was also conducted to understand the overall pattern change in student answering pattern and cyber-psychology. We calculated the pre and post average student performance for each survey.

We conducted a total of 13 surveys, 6 pre-surveys and 7 post surveys, refer table II. Play-Read-Disrupt app was performed as a demo to the class, so a pre-survey for this application was not conducted. Some of the questions posed in the survey and student responses are presented in table III. Overall, a positive outcome was observed by the usage of smartphone apps as cyber-psychological exercises. The questions in the survey were mostly 5 level likert scale, with the options as Yes (100% Confident), Yes (Fairly Confident), Unsure (50-50), No (Fairly Confident) and No (100% confident) or Strongly Agree, Agree, Neither Agree nor Disagree, Disagree and Strongly Disagree. Depending on the question the answers were allocated points from 5 to 1, where 5-correct answer, 4-partially correct answer, 3-undecided, 2-wrong but not confident answer and 1-wrong answer.

TABLE II
LIST OF SURVEYS

App	Pre	Post
Email-Lite-Scare	✔	✔
Shop-Shock-Struck	✔	✔
Quiz Your Permissions	✔	✔
Chat-Phish	✔	✔
Social-Phish	✔	✔
Play-Read-Disrupt	✘	✔
Spy-The-Trojan	✘	✘
CLASS Overall Survey	✔	✔

A comparative graphical representation of % of correct answers by students in pre and post ransomware survey is presented in Fig. 8. Questions posed in the survey are also provided for a better understanding. A positive influential growth is observed through the results obtained from the surveys. For applications Email-Lite-Scare, Shop-Shock-struck, Quiz your permissions, Social-Phish and Chat-Phish,

TABLE III
SPECIFIC QUESTION SURVEY RESULTS FROM ALL SURVEYS

Survey	Question	No (100%)		No (Fairly)		Unsure		Yes (Fairly)		Yes (100%)	
		Pre	Post	Pre	Post	Pre	Post	Pre	Post	Pre	Post
Shop-Shock-Struck	Apps available in play and apple stores are all safe to use.	40.3	**64**	29.9	20.7	16.5	1.1	9.3	11.4	4.2	3.1
Shop-Shock-Struck	Can an application change your home screen wallpaper without your knowledge?	5.2	2.1	9.4	7.3	41.7	15.7	20.9	21.9	23	53.2
Email-Lite-Scare	Can applications scare you and obligate you to buy or download their products?	1	0	0	1	2	0	28.8	2	68.2	**96.9**
Email-Lite-Scare	Can applications show false alarms/warnings?	5.1	2	7.2	1	12.3	1	42.2	17.5	32.9	**78.3**
Quiz Your Permissions	Educational apps can be granted all the permissions such as the Internet, media storage & location.	28.9	**61.9**	40.3	17.6	17.6	7.3	9.3	9.3	4.2	3.1
Social-Phish	Hackers target for phishing targets at both common man and highly reputed organizations.	0	0	2.1	0	8.3	3.1	36.1	11.4	53.7	**85.6**
Social- Phish	Phishing attacks can occur only on mobile financial transaction apps such as banking.	7.3	**33.4**	18.6	16.7	27.9	14.6	34.1	17.8	10.4	17.8
Social-Phish	A third party cannot access the details of my personal social media account without my permission.	32	**53.2**	41.3	36.5	15.5	4.2	9.3	4.2	2.1	2.1
Chat-Phish	You can save yourself from becoming a victim of Phishing by using complex alphanumeric passwords.	2.1	0	7.3	7.3	9.3	3.1	36.1	15.5	45.4	72.2

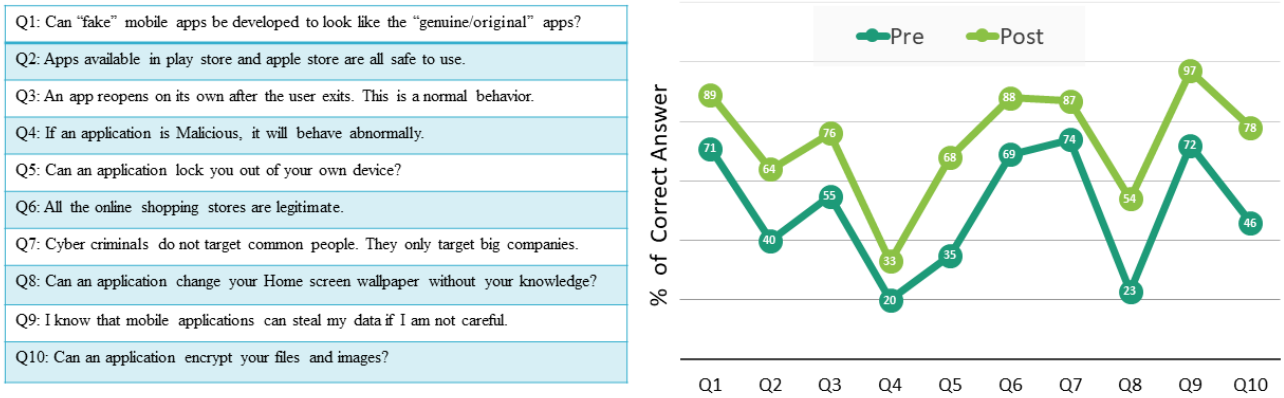

Fig. 8. Pre-Post comparison for the Ransomware Survey

the average pre-survey results were 4.228, 4.194, 4.249, 4.144 and 4.351, respectively. While the post-survey results for the applications observed were 4.499, 4.495, 4.546, 4.527 and 4.532 respectively. The overall pre-survey average is observed to be 4.233, while the overall post-survey average is 4.5198. Due to the COVID-19 restrictions, in-person summer camps were not conducted, the results obtained are all based on freshmen class of the University of Toledo, where the instructor discussed cybersecurity basics in two lecture sessions after the pre-surveys were given out.

VI. CONCLUSION

We developed Android apps focusing on malware classes – scareware, ransomware, spyware, phishing – through social networking apps and cyber-safe practices through run-time permission attacks. The apps were discussed in view of common users and attackers. With these apps, an attempt will be made to perform psychological assessment in young high school students to identify cybersecurity threats, thereby protecting them from becoming a cyberattack victim and improving their self-efficacy to pursue cybersecurity as a career. By amplifying their knowledge on defense strategies, we expect to increase the number of cybersecurity professionals successively. We will use these apps in a cybersecurity summer camp and evaluate students' understanding using popular NASA Task Load Index (NASA-TLX) assessment tool. In future, we will explore other areas of cyberattacks such as automated hacking, AI scams, and web based attacks as well.

VII. ACKNOWLEDGMENT

This project has been supported by the National Science Foundation Award #1903419 and #1903423.

REFERENCES

[1] Hackers attack every 39 seconds, May 2020.
[2] J. Clement. Biggest online data breaches worldwide 2020, Apr 2020.
[3] Rob Sobers. 110 must-know cybersecurity statistics for 2020, June 2020.
[4] Rebecca Vogel. Closing the cybersecurity skills gap. *Salus journal*, 4(2):32–46, 2016.
[5] Steve Morgan. Cybersecurity talent crunch to create 3.5 million unfilled jobs globally by 2021, Nov 2019.
[6] Yatan Pal Singh Balhara, M Harshwardhan, Rajeev Kumar, and Shalini Singh. Extent and pattern of problematic internet use among school students from Delhi: Findings from the cyber awareness programme. *Asian journal of psychiatry*, 34:38–42, 2018.
[7] Kodey S Crandall, Cherie Noteboom, Omar El-Gayar, and Kalee Crandall. High School Students' Perceptions Of Cybersecurity: An Explanatory Case Study. *Issues in Information Systems*, 20(3), 2019.
[8] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn)*, 12(1):150–158, 2018.
[9] William Crumpler and James A Lewis. The cybersecurity workforce gap. *Center for Strategic and International Studies, Washington, DC.[Online]. Available: https://www. csis. org/analysis/cybersecurityworkforce-gap*, 2019.
[10] Mansoor Iqbal. App download and usage statistics (2019), Apr 2020.
[11] Dan Goodin. Google play's malicious app problem infects 1.7 million more devices, Mar 2020.

[12] Jacqui Taylor-Jackson, John McAlaney, Jeff Foster, Abubakar Bello, Alana Maurushat, and John Dale. Incorporating Psychology into Cyber Security Education: A Pedagogical Approach. *Proceedings of Asia USEC*, 20, 2020.

[13] Marc Olano, Alan Sherman, Linda Oliva, Ryan Cox, Deborah Firestone, Oliver Kubik, Milind Patil, John Seymour, Isaac Sohn, and Donna Thomas. SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education. In *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, 2014.

[14] Peter Chapman, Jonathan Burket, and David Brumley. PicoCTF: A game-based computer security competition for high school students. In *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, 2014.

[15] Ovidiu-Gabriel Baciu-Ureche, Carlie Sleeman, William C Moody, and Suzanne J Matthews. The Adventures of ScriptKitty: Using the Raspberry Pi to Teach Adolescents about Internet Safety. In *Proceedings of the 20th Annual SIG Conference on Information Technology Education*, pages 118–123, 2019.

[16] Jason Michael Pittman and Ron Pike. An Observational Study of Peer Learning for High School Students at a Cybersecurity Camp. *Information Systems Education Journal*, 14(3):4, 2016.

[17] Minzhe Guo, Prabir Bhattacharya, Ming Yang, Kai Qian, and Li Yang. Learning mobile security with android security labware. In *Proceeding of the 44th ACM technical symposium on Computer science education*, pages 675–680, 2013.

[18] Anthony Peruma, Samuel Malachowsky, and Daniel Krutz. Providing an experiential cybersecurity learning experience through mobile security labs. In *2018 IEEE/ACM 1st International Workshop on Security Awareness from Design to Deployment (SEAD)*, pages 51–54. IEEE, 2018.

[19] Wanqing You, Kai Qian, Dan Chia-Tien Lo, Prabir Bhattacharya, Wei Chen, Tamara Rogers, Johng-Chern Chern, and Junfeng Yao. Promoting mobile computing and security learning using mobile devices. In *2015 IEEE Integrated STEM Education Conference*, pages 205–209. IEEE, 2015.

[20] Xiaohong Yuan, Kenneth Williams, Scott McCrickard, Charles Hardnett, Litany H Lineberry, Kelvin Bryant, Jinsheng Xu, Albert Esterline, Anyi Liu, Selvarajah Mohanarajah, et al. Teaching mobile computing and mobile security. In *2016 IEEE Frontiers in Education Conference (FIE)*, pages 1–6. IEEE, 2016.

[31] Minzhe Guo, Prabir Bhattacharya, Kai Qian, Chia-Tien Dan Lo, and Xi He. Enhancing the information assurance and security (IAS) in CS education with mobile-device based hands-on labs. In *Proceedings of*

[21] Hongmei Chi. Integrate mobile devices into CS security education. In *Proceedings of the 2015 Information Security Curriculum Development Conference*, pages 1–4, 2015.

[22] Kai Qian, Dan Lo, Reza Parizi, Fan Wu, Emmanuel Agu, and Bei-Tseng Chu. Authentic learning secure software development (SSD) in computing education. In *2018 IEEE Frontiers in Education Conference (FIE)*, pages 1–9. IEEE, 2018.

[23] Jean-François Lalande, Valérie Viet Triem Tong, Pierre Graux, Guillaume Hiet, Wojciech Mazurczyk, Habiba Chaoui, and Pascal Berthomé. Teaching android mobile security. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, pages 232–238, 2019.

[24] Minzhe Guo, Kai Qian, and Li Yang. Hands-on labs for learning mobile and NoSQL database security. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, volume 2, pages 606–607. IEEE, 2016.

[25] Kai Qian, Dan Lo, Hossain Shahriar, Lei Li, Fan Wu, and Prabir Bhattacharya. Learning database security with hands-on mobile labs. In *2017 IEEE Frontiers in Education Conference (FIE)*, pages 1–6. IEEE, 2017.

[26] Lei Li, Kai Qian, Qian Chen, Ragib Hasan, and Guifeng Shao. Developing hands-on labware for emerging database security. In *Proceedings of the 17th Annual Conference on Information Technology Education*, pages 60–64, 2016.

[27] Kai Qian, Chia-Tien Dan Lo, Minzhe Guo, Prabir Bhattacharya, and Li Yang. Mobile security labware with smart devices for cybersecurity education. In *IEEE 2nd Integrated STEM Education Conference*, pages 1–3. IEEE, 2012.

[28] Sandro Fouché and Andrew H Mangle. Code hunt as platform for gamification of cybersecurity training. In *Proceedings of the 1st International Workshop on Code Hunt Workshop on Educational Software Engineering*, pages 9–11, 2015.

[29] Zouheir Trabelsi, Mohammed Al Matrooshi, Saeed Al Bairaq, Walid Ibrahim, and Mohammad M Masud. Android based mobile apps for information security hands-on education. *Education and Information Technologies*, 22(1):125–144, 2017.

[30] Shaibu Adekunle Shonola and Mike Joy. Enhancing mobile learning security. *arXiv preprint arXiv:1610.06046*, 2016.
the 2014 conference on Innovation & technology in computer science education, pages 343–343, 2014.

[32] Chuan Yue. Teaching computer science with cybersecurity education built-in. In *2016 {USENIX} Workshop on Advances in Security Education ({ASE} 16)*, 2016.