# Changes in High-School Student Attitude and Perception Towards Cybersecurity Through the Use of an Interactive Animated Visualization Framework

Sai Suma Sudha*, Gabriel Castro Aguayo†, Abel R Angulo†, Jyothirmai Kothakapu*,
Quamar Niyaz†, Xiaoli Yang‡, Ahmad Y Javaid*
*EECS Department, The University of Toledo, Toledo, OH, United States
†ECE Department, Purdue University Northwest, Hammond, IN, United States
‡CS Department, Fairfield University, Fairfield, CT, United States
{ssudha, ahmad.javaid}@utoledo.edu, {gcastroa, areyesan, qniyaz}@pnw.edu, xyang@fairfiled.edu

***Abstract*—The enormous advancement of digital technology and the Internet usage have significantly improved our lives, but have threatened our security and privacy as well. Cyberattacks may have harmful long-term implications to individuals and organizations. High school students are accessible targets for various cybercrimes due to the lack of cybersecurity knowledge and cyber-safe practices. It is important that education about cybersecurity awareness and cyber hygiene practices must begin at a young age. Offering cybersecurity knowledge through interactive tutorials and game-based techniques may increase students' interest in this domain. To develop a security mindset and improve the perception and attitude towards cybersecurity, we created an interactive cybersecurity framework for high school students. Through this framework, we attempt to effectively educate students in cybersecurity through interactive animated visualization modules developed in Unity 3D engine, enabling learning of physical, software, and mathematical aspects of cybersecurity. Each topic in the visualization tool is explained in four stages including information, interaction, explanation, and assessment. Several surveys have been conducted to determine whether this framework enhances users' cognitive abilities.**

***Keywords*—cybersecurity career, awareness of cybersecurity, visualization modules, Unity 3D**

## I. INTRODUCTION

Online transactions and purchases are very common nowadays due to the recent development of web technologies and Internet usage. Users can send and receive money from their bank accounts, make purchases more quickly and securely online than in-person, and connect with friends on social media makes these tools very attractive. Although the use of technology and the Internet have improved our daily lives, they have some harmful effects on our security and privacy [1]. Many people and organizations become cybercrime victims on a daily basis. Recently, cybersecurity has gained utmost importance for organizations and nations to safeguard them against various cyberattacks. Attackers find ways to compromise credentials and private by utilizing several cyberattack techniques and tools when users carry out their routine tasks and provide information to purchase or sign up for services. Since the global epidemic began, there has been a 600% surge in all forms of cybercrime [2]. According to Cybersecurity Ventures, during the next five years, the cost of cybercrime will see an annual increase of 15%, reaching from $3 trillion in 2015 to $10.5 trillion annually by 2025 [3]. Millions of critical data records, particularly in the banking and healthcare sectors, have been compromised, and national infrastructure, businesses, and government organizations have all been the target of cyberattacks [4].

A growing concern is that today's cybercrime victims not only include organizations and high-profile personalities, but also school students. There has been around a 150% increase in the number of cyber-fraud victims who are under 21 years between 2017 and 2020. The Internet Crime Complaint Center received around 23,000 complaints in 2020 from under 21 age group individuals resulting in a loss of roughly 71M US dollars [5]. There are many educational and entertainment resources available on the Internet. Depending on their choices, teenagers may visit different websites for learning and entertainment. These resources might improve students' experience, but they can also result in specific privacy and security issues if they are not offered through trusted sources. It is important to increase students' understanding of cybersecurity issues and teach them how to protect themselves online. To educate them about safe online and technology usage habits, having them practice visually might be helpful. Students can learn various cybersecurity threats and protection using cybersecurity visualization, which can be beneficial in teaching them how to stop a harmful attack. In this paper, we discuss our interactive visualization framework developed to teach various cybersecurity concepts to high school students. This work extends our previous work [6] with the enhancement of learning modules in the framework and students' surveys to determine whether the framework has a positive impact on them for cybersecurity education.

The rest of this paper is structured into five sections. Section II discusses related works in this domain. Section III provides details of our interactive visualization framework including its design and modules. Section IV presents survey results conducted during the summer camps for the framework. Finally, the paper is concluded in Section V.

## II. Related Work

Game-based and robotic platforms are the delivery methods for cybersecurity education that have received the most attention in the past few years [7], [8]. One of the most well-known cybersecurity game is "CyberCIEGE," an interactive visualization game. The players take the roles of IT decision-makers for small enterprises in a 3D office setting [9]. The participants must make security-related judgments in several scenario-based tasks based on real-world scenarios. The ideas of encryption, patching, and DMZ is used to create the situations. A 2D decision-making game called Bird's Life teaches anti-phishing to college students and the general public [10]. Undergraduate students can learn security principles with the game security concepts with Alternate Reality Games (ARG). The scene was a course that covered the fundamentals of computer science while examining ideas from the perspective of cybersecurity [11]. Another single-player data-driven security game, Data-driven Security Game (DdSG), aims to teach inexperienced developers how to choose traditional mitigation tactics and patterns to fight against various security attack scenarios [12]. A 2D game called Pomega aims to raise people's knowledge about cybersecurity awareness. Phishing, password security, social media, mobile security, and physical security are the five cybersecurity awareness issues covered in the game [13]. A 2D game called Cyber Air-Strike aims to teach cybersecurity awareness while incorporating Bloom's Revised Taxonomy interactively. The game was created as a web-based application with the Buildbox game engine [14]. Another multiplayer card game, Security Requirement Education Game (SREG), tries to raise people's awareness of cybersecurity issues. This game was created utilizing cybersecurity expertise, a game-based approach, and security requirement engineering principles, including distinct sorts of attackers and vulnerabilities [15]. The Internet Hero game aims to teach kids between the ages of nine and twelve the social and technical bases of using the Internet. Four aspects of using the Internet are covered in the game's mini-games: emails, harmful software, social networks, and connection kinds. Players must understand these topics' core technical or civil elements to complete the games [16].

In our work, we bring the idea of interaction-based visualization into the proposed framework by using serious games in education, which actively involve students in studying security principles. The created tool will aid students in learning each subject through engaging visualization-based simulations. Additionally, the application has assessments for the student's understanding of each topic after it has been covered.

## III. Interactive Visualization Framework

### A. *Why a visualization tool?*

Our goal is to give student users a framework for visualizing various cyberattacks without requiring them to have computer science or cybersecurity expertise. Additionally, the team focused on showing consumers real-world events so that they can better comprehend assaults in their digital life and be able to prevent them. Among other things, the developed framework changed from an entertaining game to a teaching tool. Using the Unity game engine, the proposed visualization framework was developed, which works on Windows, Mac, and Linux environments. The framework's modifiability is enhanced by the engine utilized in its development thanks to its easily upgradeable application programming interface (API). Instead of making the students feel like they are in a class, the tool strives to improve their knowledge using a simple and open-ended framework they can access outside class. The primary research question that we attempted to answer was: *"How effective are interactive animated visualization modules in supporting learning of the physical, software, and mathematical aspects of cybersecurity?"* In addition, we wanted to see if there are differences in learning based on gender and/or race. We have provided the list of questions along with results in Section IV to provide a better insight. The primary goal of this visualization tool is to: a) help high school students develop a security mindset, b) allow students to learn cybersecurity fundamentals, and c) enhance interest in cybersecurity careers.

### B. *Design of Visualization tool*

The framework has four stages: (i) Information, (ii) Interaction, (iii) Explanation, and (iv) Assessment, which are all embedded as subsystems. To ensure long-term information retention, students may progress through each level developed for various cybersecurity topics in the tool. After each topic, students take a short assessment to gauge their understanding. The information stage allowed users to look over the ideas on the tool's topics. Students engaged with the tool topics through interaction, and examined the causes of the interaction section in the explanation section. After the complete evaluation, students reviewed their knowledge through a true-false and multiple-choice questions based surveys. Fig. 1 shows the flow chart of the learning module. To complete the learning of the subtopic, the user must complete the four stages included in each subtopic.

### C. *Modules of the Visualization tool*

In the cyber world, threats come in a variety of forms. Depending on the functionality and target, these attacks can be carried out via malware or other techniques to harm websites or networked systems. There are four different modules in the visualization tool, as shown in Fig. 2a: (i) Cryptography, (ii) Malware, (iii) Network Security, and (iv) Web Security.

*1) Cryptography:* Data protection and data breach prevention are both possible with cryptography. Only those who are intended to read the messages will be able to decipher them using the cryptographic keys, which makes it possible to use encrypted messages for sharing [17]. The confidentiality of the information is the main objective of cryptography, and only the intended recipient and the person who encrypts the message can read the information. In cryptography, plain and cipher text are terms used to describe different text types. Users typically need a key to encrypt and decrypt information

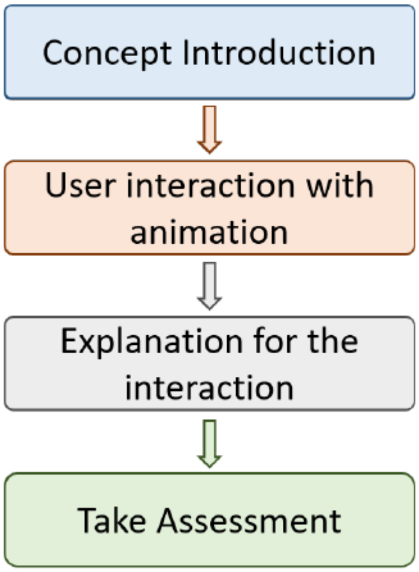

Concept Introduction
User interaction with animation
Explanation for the interaction
Take Assessment

Fig. 1: Four stages of learning in the visualization framework

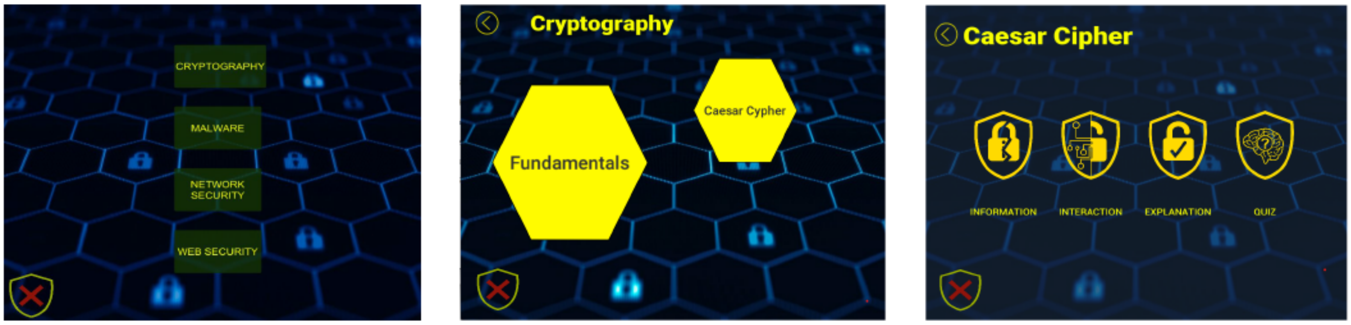
to prevent unwanted users from accessing them. However, attackers can find ways to get these keys to decipher the messages. This section discusses fundamental of cryptography concepts including encryption, decryption, and symmetric and asymmetric algorithms. Fig. 2b shows the menu of the Cryptography.

*a) Caesar Cypher:* **Information stage:** The Caesar Cipher is among the most well-known and straightforward encryption techniques. Each letter in the plain text is replaced by a letter that is located a specific number of positions farther down the alphabet in this form of substitution cipher. For example, with a left shift of 3, D would become A, E would become B, and so on. This provides Caesar Cipher information. Fig. 2c shows the sub-menu of the Caesar Cipher. **Interaction stage:** We gave students an example to help them understand the Caesar Cipher. Students successfully finished the task by following the instructions. **Explanation stage:** We go through with students for the activity they performed in the information stage. In this stage, we offer step-by-step explanations for the previous activity. **Assessment stage:** We created several questions and stored them in an XML file to evaluate student learning. During the assessment, randomly selected questions are asked to the user and the tool computes their scores.

*2) Malware:* Software intended to shut down, disrupt, seize control of computer systems or impede access to documents is called malware. Web links, emails, and external USB drives can all be used to transmit malware, and it can gain unauthorized access to a network. The victim must click a link to run the malicious file. As malware evolves, it poses a severe threat to cybersecurity that must be addressed. Update the operating system and install applications as regularly as feasible are a few crucial measures to follow to prevent malware attacks. Additionally, we should not open suspicious emails or click on strange websites. Some key ideas for malware security are explained in this section. The three sections of this module are fundamentals, keylogging, and ransomware. GUI of the Malware subtopics is shown in the Fig. 3a. It educates students to be cautious and attentive when installing apps. The students are given assessments at the conclusion to gauge their performance. The malware fundamental screen is shown in Fig. 3b.

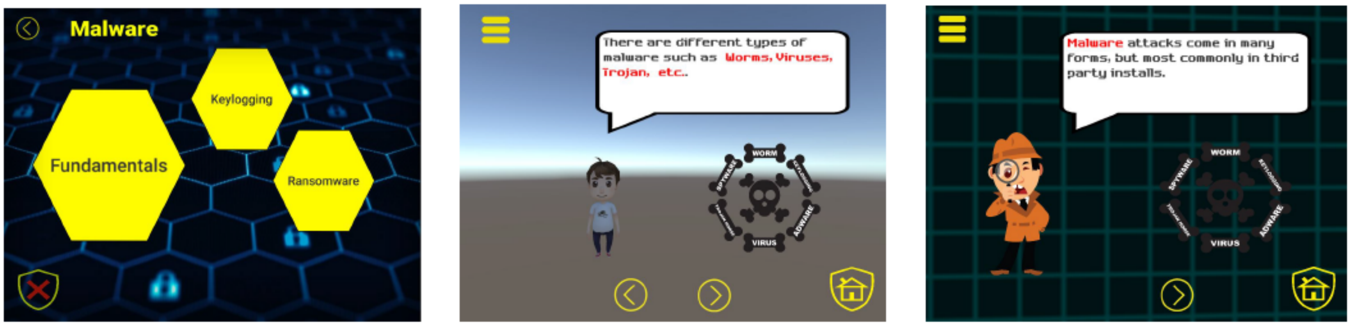
*a) Keylogging:* **Information stage:** We offer information about Keylogging malware in this section. We explain how it enters our system and how it functions and provide a few instances. An infected computer's keystrokes are recorded by keylogging malware, which communicates the recorded information to a third party. It mainly steals private data including credit card numbers or account passwords. Malicious software with keylogging functionality rapidly expands, and attackers frequently combine several types of malware to achieve their espionage goals. For instance, a keylogging incident in 2009 revealed an almost $1 million theft from Nordea, a Scandinavian bank. Emails were sent to bank customers requesting that they install an anti-spam program. A Trojan named Haxdoor was established once the package was downloaded. Keylogging functionality built into the Haxdoor program allowed for recording the information entered by bank customers. The money from the victim was then transferred to the attackers' accounts [18]. As we intend for the user to recall the topic by referring to the character, we designed a symbol to illustrate the concept of keylogging in this module. Fig. 3c shows the Keylogging Information. **Interaction stage:** A key-logger malware real-world scenario is shown. We used a smartphone example that has several apps installed. Due to the appearance of an odd app that was not previously installed, the phone will appear infected. The user will use the infected phone to reply to friends' text messages later in the lesson. An alert notifying the user that a third party can see anything being entered will appear out of nowhere. The pop-up messages show that the peculiar program remembered the messages the user had already typed. Fig. 4a shows the Keylogging Interaction. **Explanation stage:** We outline the interaction phase and detail the emergence and operation of keylogging. Additionally countermeasures are described so that users would know how to prevent these kinds of assaults. Checking the permissions users give an app to use and keeping an eye on any unknown apps are the most significant ways to prevent keylogging. **Assessment stage:** We created 5 questions randomly selected from a database of 10 questions and placed them in an XML file to evaluate student learning by computing the score. There are numerous choices for each question. The questions include the occurrence, operation, and prevention of keylogging.

*b) Ransomware:* **Information stage:** The same character is used throughout this module to maintain consistency throughout the malware family. A description of ransomware is given, along with an example of how it attacks. This malware has been advancing over time and is used to demand payment from the victims. Attackers use this malware to shut down the victim's computer or impede access to documents



(a) Main menu (b) Cryptography sub-menu (c) Caesar cipher sub-menu

Fig. 2: Various menu screens of the developed visualization framework

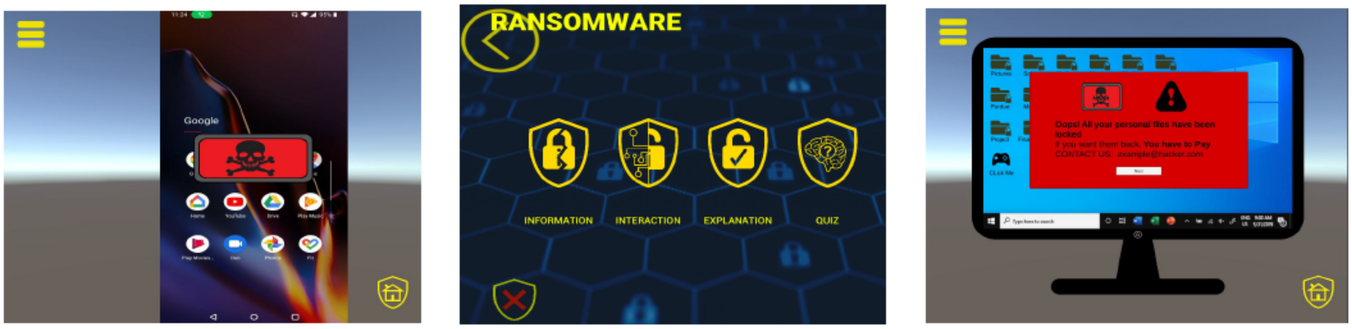


There are different types of malware such as Worms, Viruses, Trojan, etc..

Malware attacks come in many forms, but most commonly in third party installs.

(a) Subtopics in the malware module (b) Explanation stage of the malware module (c) Information for keylogging malware

Fig. 3: Malware module of the developed visualization framework



Oops! All your personal files have been locked
If you want them back, You have to Pay
CONTACT US: example@hacker.com

(a) Interactive demo of keylogging malware (b) Learning stages for Ransomware subtopic (c) Interaction stage of ransomware subtopic.

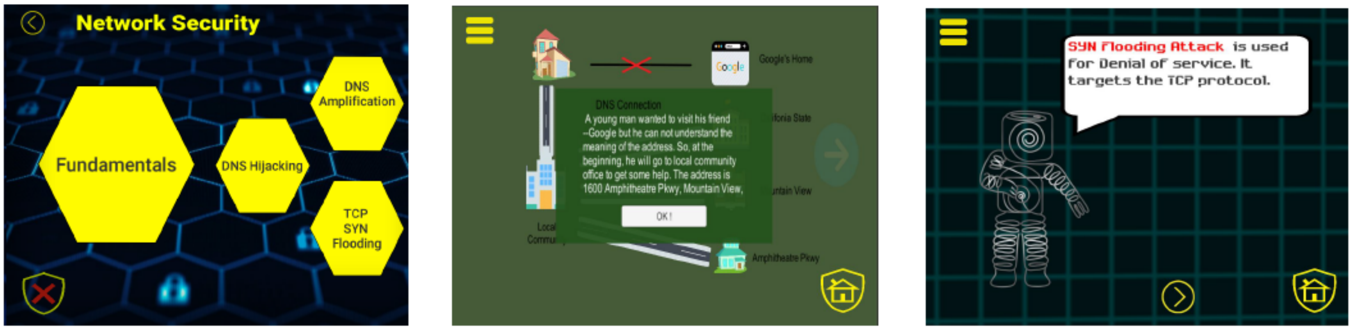
Fig. 4: Screenshots for Keylogging and Ransomware sub-modules

using various techniques. After a malware attack penetrates a machine or system, all personal files are locked or the victim's computer's functionality is blocked. Fig. 4b shows the Ransomware menu. Ransomware then shows a notification requesting money to unlock data and restore functionality [19]. **Interaction stage:** This malware will prompt a view of the user's PC with several directories. The instructions will appear in a dialogue box. Once the executable file is clicked, the user's folders will be encrypted. The user's folders will be encrypted once the executable file is clicked. This illustration demonstrates how ransomware malware functions when it is activated. The user will receive a final message informing them that all the folders are encrypted and that a ransom fee is required to unlock them. The majority of attacks of this kind target computer hardware. Each animation will briefly explain the ransomware attack in the interactive game. The information module's same objects and script are used. Fig. 4c shows the Ransomware Interaction. **Explanation stage:** A ransomware visualization attack based on the May 2017 WannaCry virus, was utilized for the explanation portion. It was categorized as a global cyberattack and used a breach created by the US National Security Agency to target systems running the Microsoft Windows operating system. Before the WannaCry assault, the EternalBlue exploit was made public, and Microsoft made an update available that included a security fix to prevent the EternalBlue breach. However, many businesses and people were vulnerable to the attack since their operating systems were out of the current. Cybercriminals initially requested $300 in bitcoins, then increased their demand to $600. If the ransom were not paid within three days, the victims' files would have been irreversibly lost. Even when one company paid the ransom, their data was not returned. Therefore, in the section on interaction, we describe how ransomware takes advantage of the user. A few countermeasures were also described for the users to be aware of this issue. Users must make a backup of their files. **Assessment stage:** We produced 5 questions, which were taken randomly from a database and saved in an XML file to score student learning. There are numerous choices for each question, and a test on ransomware's operation and prevention was given to the learner.

*3) Network Security:* The largest network in the world is the Internet, a network of networks. Monitoring, preventing, and defending against improper activity across the network are all parts of network security. The network security procedure prevents hackers from using the network for nefarious purposes. To attack networks, adversaries frequently trick domain name system servers into thinking that users have arrived at the URL they entered into a web browser. Some typical networking assaults can cause a Denial of Service, rendering a legitimate website unable to serve users. We have a section on the basics that explains what a network is, what devices are connected to it, and what protocols are used. It also contains a quiz to test the student's comprehension and aid in understanding network dangers. The user must pass the foundational examination to access the network security subtopics. The basics of network security are explained to the while unlawful access is discussed. This module is divided into the following sections: Fundamentals, DNS Hijacking, DNS Amplification, and TCP SYN Flooding, the tool explains the fundamentals of these concepts. Fig. 5a shows the menu screen of Network Module.

*a) DNS and DNS based attacks:* **Information stage:** Humans have trouble remembering IP addresses, but every host on the internet has one that may be used to access a website. For this reason, each host is given a name to aid in memory. A service is used to change the host names into IP numbers. It established a system known as Domain Name System (DNS). It changes the IP addresses to the host names. DNS is based on a hierarchy. The browser checks its cache to see if it already has the user's IP address when they attempt to access a website. It can be used if the IP address is found. The website will submit a request to the neighborhood DNS server if the data is missing. The IP address will be returned if the information is present on the local DNS server. If not, the request will go to the root server. One of the top-level domain (TLD) servers will get a notification from the root server with information about the TLD of the website. The TLD server will receive the request and respond with the address for the website's authoritative name server. The traditional name server will then receive the request from the local DNS server asking for the website's IP address. Generally speaking, this procedure will enable visitors to access websites. When DNS servers are misused, there are consequences. Attackers can sabotage the DNS connection to accomplish their objectives, such as man-in-the-middle contacting other servers that may have information about it and denial of service, as well as keep looking until they locate it. Fig. 5b: shows the DNS Interaction. **Interaction stage:** The same steps as the DNS process are used in the DNS amplification assault, except, in this case, an outsider (attacker) will pretend to be Bob and repeatedly request Google's address, resulting in Bob receiving a lot of emails as replies. When Bob opens all of his mail, his home will be overrun by responses, and he will feel overwhelmed. In a DNS hijacking encounter, a third party (the attacker) will drive Bob to a haunted house by giving him a shortcut to Google's URL. **Explanation stage:** In contrast to the information template, we choose a different strategy. We give examples of both a DNS attack and the DNS process. During a DNS amplification attack, the attacker will send several requests to the server using the victim's IP address. Therefore, the victim will receive a copy of every server answer. As a result of being inundated with many responses, the victim will be prevented from delivering services. In DNS hijacking, the DNS server is deceived, which causes victims to be redirected to false websites. **Assessment stage:** Depending on the type of DNS assault the user is viewing, we employ multiple choice questions to assess the user's knowledge of DNS connections, amplification, and hijacking attacks. As we intend to emphasize to the user, a DNS connection works; as a result, they will readily comprehend the attacks.

*b) TCP and SYN Flooding attack:* **Information stage:** The transmission control protocol is a connection-oriented transport protocol that many applications, such as email and the web, frequently employ because data can be transferred reliably and accurately.Before any data is transmitted, a three-way handshake establishes a connection between the sender and the destination. For instance, a client must first establish a relationship via a three-step, three-way handshake to view web pages from a server. First, the client sends an SYN message to the server to seek synchronization or a connection. Second, the server will inform the client that the request has been acknowledged by providing an SYN-ACK message. The client then provides an ACK message in response.Following that, the client and server create a connection. Denial-of-service attacks like SYN flooding target the server to stop the creation of new connections. The half-open SYN connection message from the client will be buffered by the server throughout the three-way handshake and erased after the connection has been established. A SYN flooding attack aims to overload the server's buffer to prevent it from accepting genuine client requests. The attacker repeatedly requests connections in step one of the three-way handshake from fictitious, nonexistent IP addresses to fill the server's SYN buffer. Step 2 involves the server sending acknowledgments to each IP address and then waiting for replies. Due to nonexistent IP addresses and a full SYN buffer, the server does not get any answers. As a result, the server cannot reply to legitimate client requests.



DNS Connection
A young man wanted to visit his friend --Google but he can not understand the meaning of the address. So, at the beginning, he will go to local community office to get some help. The address is 1600 Amphitheatre Pkwy, Mountain View,

SYN Flooding Attack is used for Denial of service. It targets the TCP protocol.

(a) Subtopics in network security module.
(b) Example of DNS attack's methodology
(c) Information for TCP SYN flooding

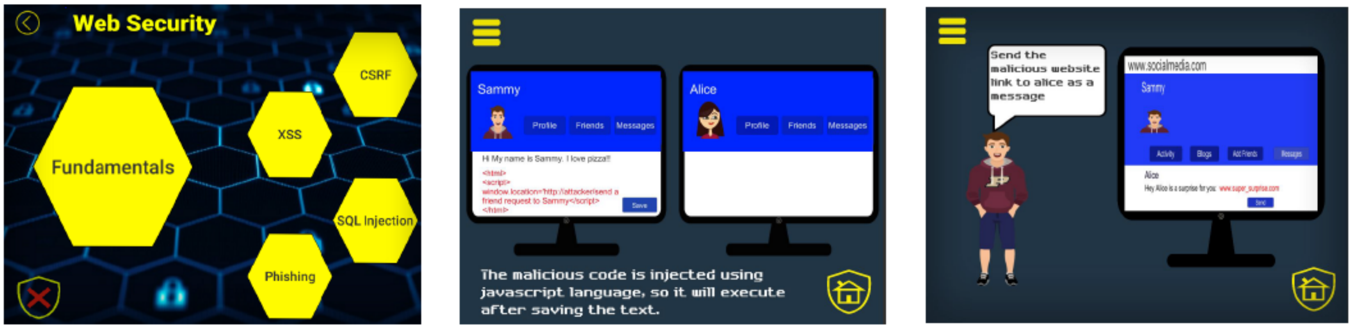
Fig. 5: Screenshots for Network Security module

Fig. 5c shows the TCP Information. **Interaction stage:** In this stage,the TCP process is explained first. A dialogue game was used in the visualization to represent the interaction between two characters that are striving to become friends. Bulbasaur represents the server, and Pikachu is the client. The friend request was be sent by Pikachu first, and Bulbasaur responds to the request and notifies the pals that they have been accepted. When Pikachu finally confirms the request, Bulbasaur and Pikachu become buddies. An unfamiliar figure named Koffing (the attacker) was introduced in the flooding attack. He tried to keep Bulbasaur (the server) busy to prevent him from accepting new friend requests. Koffing sent the initial friend request (first step). Bulbasaur informed the friends that they have approved the request whenever they receive a response (second step). To sum up, Koffing won't grant. Bulbasaur therefore waited for Koffing's approval before making pals. Due to Bulbasaur's continued association with Koffing, their friendship didn't flourish. **Explanation stage:** This stage gave a step-by-step explanation of how to establish a TCP three-way handshake connection. A text box described how the client and server is used for commnication to display. An SYN buffer also presented on the server, saving the connection requests and deleting them once the connection has been established. **Assessment stage:** Before introducing the attack principles in this module, we want to evaluate the user's understanding of fundamental TCP concepts, such as how a three-way handshake connection functions. Additionally, since SYN flooding attacks target servers that offer customers any form of service, we want users to be able to recognize them as denial-of-service attacks.

*4) Web Security:* This framework's primary focus is website security assaults, including phishing, cross-site scripting attacks, cross-site request forgeries, and SQL injection. For the students to better understand website security attacks, we have a foundations portion that explains what a website is, what apps are included in a website, and what website vulnerabilities are. The section ends with a test to see how well students comprehended it. The student must complete the foundation exam to access the web security subtopics. Fig. 6a: shows the menu screen of Web Security.

*a) Cross-Site Scripting (XSS):* **Information stage:** Before presenting the XSS assault, certain earlier concepts are discussed at this level. The programming language JavaScript, utilized in web development, is used in cross-site scripting assaults [20]. JavaScript can be used to inject malicious code into a website that is susceptible to XSS attacks. The code's functionality will impact any user that visits the vulnerable website when it is loaded with malicious content.We developed a figure representing someone attempting to use an XSS attack to add friends to their social media accounts. Our engagement module will feature a social media scenario. This illustration was taken from SEED labs [21]. **Interaction stage:** Without Alice's permission, the fictional Sammy attempted to add her as a friend on social media. The user aided Sammy in carrying out an XSS attack. He first entered the harmful code on his profile and hide it for this process. Each time a user entered Sammy's profile, the code was triggered. Sammy encouraged Alice to view his profile at this point. When Alice viewed his profile, her account automatically sends Sammy a friend request without her knowledge. The user can view the animations for both sides thanks to this framework, which displays both social media profiles (those of the victim and the offender). XSS Interaction Visualization is shown in Fig. 6b. **Explanation stage:** The attacker's approach to exploiting the vulnerability is displayed in the explanation portion. A website must be insecure and allow visitors to inject JavaScript code to employ XSS. Sammy performed the attack after determining whether the website was vulnerable. Once a flaw has been identified, Sammy injects malicious JavaScript code to force users to add him as a buddy. Visitors to his social networking pages will run his harmful malware. As a result, they will unknowingly send Sammy friend requests. The attack's execution is explained in this module's interaction section. **Assessment stage:** We test the student on the execution of the attack using XSS-related questions. The concepts of JavaScript, Web servers, same-site requests, and cross-site requests were evaluated using multiple-choice questions.

*b) Cross-Site Request Forgery:* **Information stage:** CSRF is introduced. When a victim accesses a malicious website, the request is sent to a weak website, which then carries out unwanted actions. We explain how CSRF operates and



Hi My name is Sammy. I love pizza!!

```
<html>
<script>
window.location='http://attacker/send a
friend request to Sammy</script>
</html>
```

The malicious code is injected using javascript language, so it will execute after saving the text.

Alice

Hey Alice is a surprise for you: www.super_surprise.com

(a) Subtopics in web security module

(b) Example of XSS attack

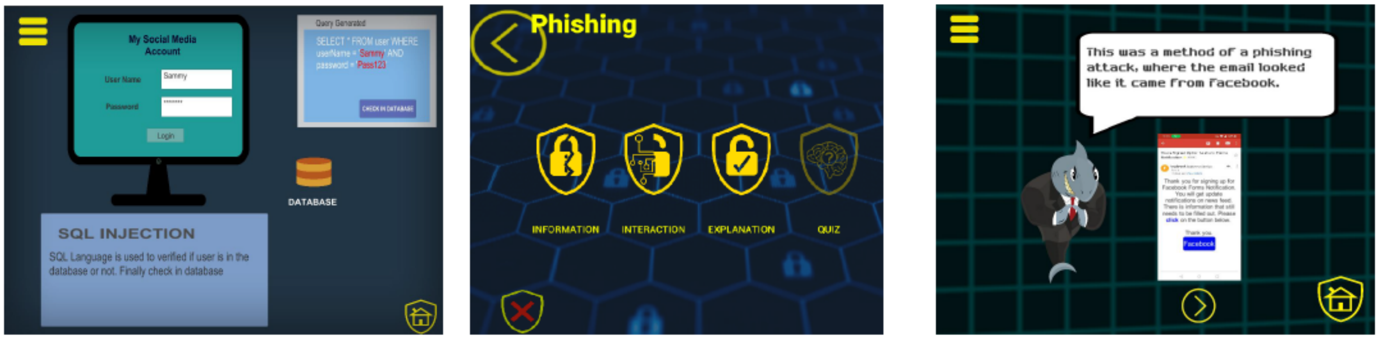
(c) Interaction of CSRF attack

Fig. 6: Screenshots of Web Security module

how it deceives trustworthy websites. **Interaction stage:** In interaction stage, the first implementation will be the same as the information section. There will be a character from the animation and dialogue messages. Along with the conversation, brief animations will allow the user to engage while following the instructions. In this cartoon, Sammy attempts to add Alice as a friend on social media against her will. The user will assist Sammy in conducting a CSRF attack. Sammy will first obtain the URL from the risky social media, and Sammy will request a friend from an outside account to get the produced URL. Sammy will then insert the URL-containing malicious code into a third-party website. When the malicious code is activated, Sammy will receive a friend request. Finally, he will message Alice on social media with the link to the malicious website. When Alice clicks the link, an automatic friend request will be sent to Sammy without Alice's knowledge. The interaction visualization for CSRF is shown in Fig. 6c. **Explanation stage:** The CSRF interaction is described at the explanation stage. Sammy had to add Alice as a friend first. Therefore, Alice's social media was deceived via CSRF. In this phase, the CSRF attack procedure was described using a social media attack as an example. In the explanation section, countermeasures were also illustrated to show users how to prevent this website attack. **Assessment stage:** Before the attack, we examined the user's understanding of web applications with the CSRF evaluation questions. Additionally, the user is tested on countermeasures using the explanation section's concepts.

*c) SQL Injection:* **Information stage:** Using SQL injection technique, malicious SQL queries can be injected into a website's database to alter it. This section includes details on what SQL can performed and some fundamental SQL queries that will help the user comprehend how SQL injection operates. We offered guidance on how users can identify whether a website is susceptible. **Interaction stage:** This interaction will demonstrate how an attack operates and affects a website database. A sequence of animations will be shown to the user explaining how to perform SQL injection to authenticate a website login. The username and password, in this instance, are unknown. The user will initially be required to enter random information on the login website, and a few SQL characters will then be used. A few queries were utilized to access the website without knowing the username and password. Fig. 7a shows the interaction screen of SQL Injection. **Explanation stage:** This stage explains how an attack was carried out and how to avoid attacks. To help the user understand SQL injection, some typical SQL queries used in the interaction component are also presented. **Assessment stage:** To assess user learning at this level, we produced 5 questions drawn randomly from a database stored in an XML file. Each inquiry has numerous choices.

*d) Phishing:* **Information stage:** We define phishing, describe how it operates, and discuss prevention measures. A pervasive assault is phishing, which allows the attacker to take information from victims directly in front of them. Fig. 7b shows the menu screen of Phishing. Typically, it is sent in an email that appears genuine but links to a bogus website. They may also arrive via various channels, such as text messages or software downloads. The attacker can take the victims' information once they have entered it. A fake email can be identified by its email address or by scanning the message for anomalies. Fig. 7c shows the Phising Visualization. **Interaction stage:** This website attack will display an animation of how phishing emails can harm a device. The phone will receive an email at the beginning of the animation, and the user will open the email asking them to update their Facebook password. Once clicked, a phony Facebook website will appear for the user. After entering a username and password, the victim will suddenly have their information taken. Consequently, this animation will demonstrate how a victim of phishing can quickly lose personal information. This animation consists of five screens that need to be displayed. One image appears on each screen, and a button enables the user to switch to other screens. Additional input field objects that allow typing can be found on the fourth screen. On the last screen, we used an animator to display a pop-up message to inform the viewer that the attack happened. **Explanation stage:** We described how typical phishing attacks are carried out and how to avoid them. Additionally, a few techniques were discussed from the perspective of the interface to help the user understand what phishing is. **Assessment stage:** To assess user learning at this level, we produced five questions



Query Generated

SELECT * FROM user WHERE userName = Sammy AND password = Pass123

CHECK IN DATABASE

SQL INJECTION

SQL Language is used to verified if user is in the database or not. Finally check in database

This was a method of a phishing attack, where the email looked like it came from Facebook.

(a) SQL Injection demo (b) Learning stages of Phishing subtopic (c) Explanation of Phishing attack

Fig. 7: Screenshots of SQL Injection and Phishing attacks in web security

drawn randomly from a database stored in an XML file. Each inquiry has numerous choices.

## IV. Results

The findings were based on pre-and post-surveys completed before and after module sessions. The students that attended the University of Toledo and Purdue University Northwest summer camps in 2022 are the source of the survey's data. Surveys were taken from roughly 30 students during the one-week camp. Various surveys were conducted in pre/post format for the topics covered in the framework as well as lectures and other hand-on activities. Four topics included the topics in the framework, and the other two were general cybersecurity and students' attitudes and perceptions about cybersecurity. The results of Internet Security based on gender are mentioned, as this was explained during the lecture sessions to the students. This work specifically deals with the analysis of perception, attitude related and Internet security based on gender surveys that are discussed in more detail in the following subsections. And in order to provide the results more readable to the user, the average of the questions are mentioned below in every result.

### A. General Cybersecurity Attitude

We used this visualization tool to help the students develop a cybersecurity mindset. This set of questions focused on general attitude towards cybersecurity and attempted to evaluate the improvement in that domain, using 19 questions. We conducted a survey using a 5-point Likert scale as shown in Table I. The results of the survey is shown in Fig. 8. Results show that except the two questions that deals with security of smartphones with biometric password and phishing, all other attitude related questions showed improvement. It is possible that the subject matter was not clear to students in terms of the use and advantages of biometric security. This is one aspect that was not covered in the visualization tool, and needs to be addressed through other parts of the learning framework, such as lecture slides.

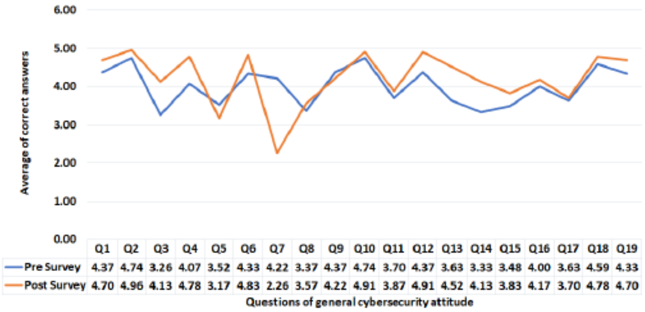


Fig. 8: Question-wise average of Cybersecurity Attitude pre/post survey (on a scale of 0-5)

### B. General Cybersecurity Perception

The students' perceptions of cybersecurity have become crucial. We surveyed students' perceptions about general cybersecurity. To assess the student's knowledge, we used a 5-point Likert scale. Fig. 9 display the outcomes of the students cybersecurity perception and Table II shows the questions mentioned in the cybersecurity perception survey, which had 11 questions. The results indicate that there was improvement on 9 out of 11 questions. It is possible that the material didn't provide clarity on those two remaining questions that dealt with the level of information accessible to ISPs and use of https.

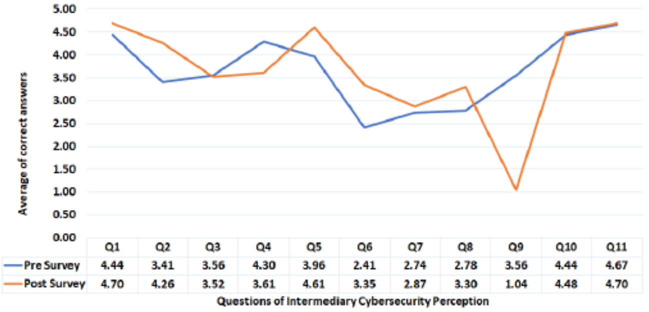


Fig. 9: Question-wise average of Cybersecurity Perception pre/post survey (on a scale of 0-5)

TABLE I: Cybersecurity Attitude Questions mentioned in the survey

| | |
|---|---|
| 1 | I think that cyberattacks can happen to me in day-to-day life. |
| 2 | It is useful for me to be aware of various cyberattacks that may target me while I am using the Internet. |
| 3 | All messages I send and receive using my electronic devices (phone, laptops, tablet, etc.) are secure. Other than me and the receiver, no one can read them. |
| 4 | It is a good practice to use a single password for all of my accounts. It's easy to remember and I don't need to write it down, hence, more security. |
| 5 | Phishing attacks can only happen on the Internet. |
| 6 | It is safe to use online banking through a public and free Wi-Fi network (e.g. in coffee shops, airports, etc.). |
| 7 | If my smartphone has a biometric password (fingerprint, facial recognition, etc.), no one can hack it. |
| 8 | If I have a problem with my phone, I usually assume that the device settings have been changed. |
| 9 | All cyberattacks are aimed at stealing money. |
| 10 | This is a strong password "strongpassword". |
| 11 | Spending less than 30 minutes a day on the Internet will save me from becoming a victim of cyberattacks. |
| 12 | It is not safe to click on the hyperlinks in a spam email. |
| 13 | If I receive a notification to upgrade my mobile app, I will update it by clicking on the notification and following the instructions without having to waste my time checking with the App Store or the Play Store. |
| 14 | If available, I always connect to a public and free Wi-Fi connection and browse the internet. |
| 15 | It is good to share the information about my day-to-day activity on social media with my friends and family. |
| 16 | It is safe to save my university login credential on my school lab computer. |
| 17 | If I do not share my password, my account will be safe. |
| 18 | It is okay to respond to spam messages or emails. |
| 19 | Saving your social security number in your phone contacts or notes is very much safe and easier to fetch when required. |

TABLE II: Cybersecurity Perception Questions

| | |
|---|---|
| 1 | Two-step authentication or multi-factor authentication is necessary to protect all my accounts. |
| 2 | Voice recording apps on your phone require access to the camera to enhance its functionality. |
| 3 | Cyberbullying occurs when you talk to strangers. |
| 4 | Information that we provide through private/incognito browser windows/tabs while browsing Internet can be accessed by internet service providers (ISPs). |
| 5 | According to Cryptography, encrypted messages cannot be decrypted. |
| 6 | I frequently update my password to prevent security issues. |
| 7 | It is safe to use an administrator account on desktops and laptops. |
| 8 | The antivirus and security system on your laptop will protect you from cyber-attacks. |
| 9 | A website link (URL) that starts with "http" is safer compared to the ones that start with "https." |
| 10 | Downloading antivirus from unknown sources is not reliable and can damage your laptop/computer. |
| 11 | If your phone is locked due to a cyber-attack and the attacker asks for money to unlock your mobile, you pay the attacker, and your smartphone will be unlocked instantly. |

TABLE III: Cybersecurity Learning Questions

| | |
|---|---|
| 1 | I find it difficult to identify a cyberattack. |
| 2 | I can immediately identify whether a website is secure. |
| 3 | I find that reading articles and understanding them is an effective way to learn about cybersecurity. |
| 4 | I cannot learn cybersecurity on my own, without regular course work at school. |
| 5 | To understand cybersecurity, I discuss it with my friends and other students. |
| 6 | Reading blogs on internet safety and understanding them saves me from cyberattacks. |
| 7 | There is typically only one right approach to solve any cyber-attack. |
| 8 | Please rate your knowledge in cybersecurity. |
| 9 | I am interested in cybersecurity for my daily technology use. |
| 10 | I am interested in pursuing cybersecurity as a career. |

### C. Cybersecurity Learning Perception

The students' perceptions of cybersecurity learning is also essential and indicates how they learn about this topic and try to stay up to date. We surveyed students' perceptions about cybersecurity learning through the 10 question-survey. To assess the student's knowledge, we used a 5-point Likert scale. Fig. 10 display the outcomes of the students cybersecurity perception and Table III shows the questions mentioned in the cybersecurity learning perception survey. The results indicate students agree that although reading from blogs and online resources is important, they need external help to learn about cybersecurity and they agree that other students at their level (friends) might not have the expertise needed (Q4-6). In addition, there was a huge improvement in the average score in terms of overall knowledge of cybersecurity after the camp. This is clearly the most positive result of this work.

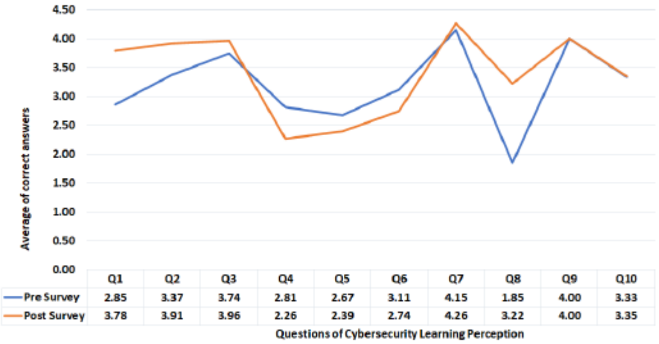


Fig. 10: Question-wise average of Cybersecurity Learning Perception pre/post survey (on a scale of 0-5)

### D. Internet security

We explained on the types of internet attacks such as TCP, DNS and their defense tools during the lecture sessions. The results were evaluated as "1" for correct answers and "0" for wrong answers. The results are shown in the Fig. 11, this clearly shows that there is an improvement on the Internet security concepts and the results for male participants were good compared to female participants. There is also scope for increasing the quality of the Internet security lecture sessions further.

## V. Conclusion

The principal objective of this initiative is to increase cybersecurity awareness among high school students by fostering a security mindset. We created a visualization tool to help with this so that the students can interactively learn cybersecurity and build a cybersecurity attitude towards the use of technology. In 2021 and 2022, we held the summer camps at Purdue University Northwest and the University of Toledo for high school students. Pre/Post-survey analysis shows that students were pleased with the module and the module had a positive impact on student learning. The survey data is

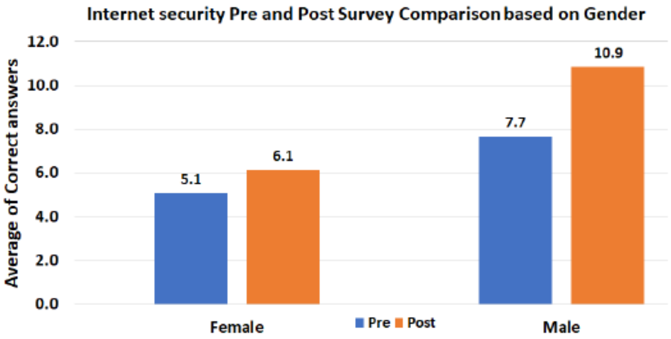


Fig. 11: Internet security Pre and Post-Survey Comparision based on gender

collected from the students who participated the summer camp. For a core cybersecurity concept, such as cryptography, the improvement was quite visible in the results, across the board. This progress can be attributed to the mathematical nature of the subject; the high school students foundational knowledge of mathematics is sufficient. On the aspects, such as perception and attitude towards cybersecurity and learning in this domain, improvements are visible in many aspects. Clearly, there is a scope of improvement on several aspects that may further enhance the quality of instruction and learning through the use of this tool.

## Acknowledgement

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

## References

[1] T. Live, “Technological influence on society.” https://tradebuzz.live/share-marketing/technological-influence-on-society/, 10 2022. Accessed Oct 20, 2022.

[2] J. Firch, “10 cyber security trends you can’t ignore in 2021.” https://purplesec.us/cyber-security-trends-2021/, 04 2021. Accessed Nov 22, 2022.

[3] S. Morgan, “Cybercrime to cost the world $10.5 trillion annually by 2025.” https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/, 11 2020. Accessed Nov 22, 2022.

[4] M. E. Johnson and N. Willey, “Usability failures and healthcare data hemorrhages,” *IEEE Security & Privacy*, vol. 9, no. 2, pp. 35–42, 2010.

[5] S. O’Brien, “Tech savvy teens falling prey to online scams faster than their grandparents.” https://www.cnbc.com/2021/08/10/tech-savvy-teens-falling-prey-to-online-scams-faster-than-their-grandparents.html, 8 2021. Accessed Feb 25, 2023.

[6] G. C. Aguayo, “An introductory visualization aid for cybersecurity education,” in *15th International Conference on Frontiers in Education: Computer Science and Computer Engineering,(FECS 19)*, 2019.

[7] M. Olano, A. Sherman, L. Oliva, R. Cox, D. Firestone, O. Kubik, M. Patil, J. Seymour, I. Sohn, and D. 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.

[8] O.-G. Baciu-Ureche, C. Sleeman, W. C. Moody, and S. 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*, pp. 118–123, 2019.

[9] C. E. Irvine, M. F. Thompson, and K. Allen, “Cyberciege: gaming for information assurance,” *IEEE Security & Privacy*, vol. 3, no. 3, pp. 61–64, 2005.

[10] P. Weanquoi, J. Johnson, and J. Zhang, “Using a game to improve phishing awareness,” *Journal of Cybersecurity Education, Research and Practice*, vol. 2018, no. 2, p. 2, 2018.

[11] T. Flushman, M. Gondree, and Z. N. Peterson, “This is not a game: Early observations on using alternate reality games for teaching security concepts to {First-Year} undergraduates,” in *8th Workshop on Cyber Security Experimentation and Test (CSET 15)*, 2015.

[12] D. E. H. Løvgren, J. Li, and T. D. Oyetoyan, “A data-driven security game to facilitate information security education,” in *2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion)*, pp. 256–257, 2019.

[13] V. Visoottiviseth, R. Sainont, T. Boonnak, and V. Thammakulkrajang, “Pomega: Security game for building security awareness,” in *2018 Seventh ICT International Student Project Conference (ICT-ISPC)*, pp. 1–6, IEEE, 2018.

[14] J. Bhardwaj, “Design of a game for cybersecurity awareness,” 2019.

[15] A. Yasin, L. Liu, T. Li, J. Wang, and D. Zowghi, “Design and preliminary evaluation of a cyber security requirements education game (sreg),” *Information and Software Technology*, vol. 95, pp. 179–200, 2018.

[16] F. Kayali, G. Wallner, S. Kriglstein, G. Bauer, D. Martinek, H. Hlavacs, P. Purgathofer, and R. Wölfle, “A case study of a learning game about the internet,” in *International Conference on Serious Games*, pp. 47–58, Springer, 2014.

[17] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 2018.

[18] T. Olzak, “Keystroke logging (keylogging),” *Adventures in Security, April*, vol. 8, pp. 1–6, 2008.

[19] Q. Chen and R. A. Bridges, “Automated behavioral analysis of malware: A case study of wannacry ransomware,” in *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pp. 454–460, IEEE, 2017.

[20] D. Flanagan, *JavaScript: the definitive guide*, vol. 1018. O’reilly, 2006.

[21] W. Du, “Seed labs: Using hands-on lab exercises for computer security education,” in *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*, pp. 704–704, 2015.