Oct 23rd, 3:00 PM - 3:30 PM

A Survey of Serious Games for Cybersecurity Education and Training

Winston Anthony Hill Jr.
North Carolina Agricultural and Technical State University, wahill@aggies.ncat.edu

Mesafint Fanuel
North Carolina Agricultural and Technical State University, mesafintfanuel2010@gmail.com

Xiaohong Yuan
North Carolina Agricultural and Technical State University, xhyuan@ncat.edu

Jinghua Zhang
Winston-Salem State University, zhangji@wssu.edu

Sajad Sajad
North Carolina Agricultural and Technical State University, skhorsandroo@ncat.edu

Abstract

Serious games can challenge users in competitive and entertaining ways. Educators have used serious games to increase student engagement in cybersecurity education. Serious games have been developed to teach students various cybersecurity topics such as safe online behavior, threats and attacks, malware, and more. They have been used in cybersecurity training and education at different levels. Serious games have targeted different audiences such as K-12 students, undergraduate and graduate students in academic institutions, and professionals in the cybersecurity workforce. In this paper, we provide a survey of serious games used in cybersecurity education and training. We categorize these games into four types based on the topics they cover and the purposes of the games: security awareness, network and web security, cryptography, and secure software development. We provide a catalog of games available online. This survey informs educators of available resources for cybersecurity education and training using interactive games.

Keywords: Serious games; Game-based Learning; Cybersecurity;

Location

Zoom Session 1 (Main Papers Track)

Disciplines

Educational Technology | Information Security | Online and Distance Education | Technology and Innovation

INTRODUCTION

In recent years, cybercrimes such as financial fraud, identity theft, phishing attacks, and denial of service attacks have become more prevalent. Therefore, it is critically important to increase the number of professionals equipped with cybersecurity knowledge and skills.

Serious games have been developed to teach various cybersecurity topics, including security awareness, network and web security, cryptography, and secure software engineering. Serious games allow users to play out subject-related scenarios in an in-game virtual environment. Studies have shown that student retention of subject matter increases when instructor introduce gamification features to course material. (Krause , 2015)

In this paper, we surveyed the current state of serious games used for teaching cybersecurity topics. The methodology for gathering the games was searching the Google Scholar Database and the WorldCat Discovery Database for papers containing the terms “Cyber Security Games,” “Game-Based Learning,” and “Cyber Security Game Frameworks.” The search intended to discover documents in the years 2018-2019, but some older manuscripts were selected because they were well-built and had positive evaluation results. These games have audiences ranging from K-12 students, undergraduate and graduate students in academic institutions, and professionals in the cybersecurity workforce. We briefly describe each game and provide a catalog of available online games for teaching cybersecurity topics.

The organization of the remainder of the paper is as follows: Section II introduces the games according to the four categories of topics they cover, Section III presents the catalog of the games available online, Section IV discusses these games, and Section V concludes the paper.

GAMES FOR CYBER SECURITY EDUCATION AND TRAINING

In this section, we categorize the games available for cybersecurity education and training in four types according to the topics covered by the games: Security Awareness, Cryptography, Network and Web Security, and Secure Software Engineering. Table 1 shows the games that fall into these categories.

Categories	Games
Security Awareness	**Threats and Protection:** Pomega (Visoottiviseth et al., 2018), Cyber Air-Strike (Bhardwaj, 2019), Security Requirement Education Game (SREG) (Yasin et al., 2018), Cyber Detective (Lopes et al., 2018), Google's Interland (Seale & Schoenberger, 2018), Attacker-Centric Gamified Approach (Adams & Makramalla, 2015), Internet Hero (Kayali et al., 2014) **Anti-Phishing:** What.Hack (Wen et al., 2019), Bird's Life (Weanquoi, 2018), Phishing Educational Game (Arachchilage & Hameed, 2017), Security Concepts with Alternate Reality Games (Flushman et al., 2015) **Device Security: Be Aware! (Sharma et al., 2019)** **Privacy:** What Can Go Wrong (Zargham et al., 2019), (Smart)Watch Out! (Williams et al., 2019), Make My Phone Secure! (Bahrini et al., 2019)
Network and Web Security	The Security Protocol Game (Hamey, 2012), Internet Security Game by NGSEC Systems (Ariyapperuma & Minhas, 2005), DDoS (distributed denial of service) Attack-Cyber Attacks (Johnson et al., 2018), SSETGami (Suarez et al., 2017)
Cryptography	Quasim (Vadla et al., 2018), Cryptography 3D Escape Game (Deeb & Hickey, 2019)
Secure Software Engineering	Counter Measures (Jordan et al., 2011), Data-Driven Security Game (Løvgren et al., 2019)

Table 1: Games in Categories

Security Awareness Games

This section introduces the games on security awareness. Games for teaching security awareness are categorized into three types: Threats and Protection, Anti-Phishing, and Device Security and Privacy.

Games That Teach Threats and Protection

Pomega (Visoottiviseth et al., 2018) is a 2D game that intends to promote cybersecurity awareness knowledge. The game was built using the Unity 3D game engine. The game implements a multi-user login system and is translated in both English and Thai. The game covers five cybersecurity awareness topics, which are phishing, password, social network, mobile security, and physical security. Users were motivated to finish the game because, after the game, users would receive a certificate. Also, certificates are awarded to users after they complete a topic. The game uses an online database server to store user data, which includes scores and progress. Additionally, other users' progress is displayed on the hall of fame page, which serves as a leader board. Three user groups evaluated the game. The results of the evaluation revealed that all users could gain higher post-test scores than pre-test scores, and most users were content with the game story and interface.

Cyber Air-Strike (Bhardwaj, 2019) is a 2D game that aspires to teach cybersecurity awareness in an interactive manner integrating Bloom's Revised Taxonomy. The game is a web-based application that was built using the Buildbox game engine. The game deals with cybersecurity awareness topics of malware attacks, phishing attacks, password hacking, virus, and unauthorized data. The gameplay is the users must travel the furthest distance while protecting their plane from the cybersecurity attacks, and users can avoid the enemies or employ allies. The game has not been tested with actual players.

Security Requirement Education Game (SREG) (Yasin et al., 2018) is a multiplayer card game that aims to improve cybersecurity awareness. This game was built using cybersecurity knowledge and a game-based technique combined with security requirement engineering concepts such as attacker types as well as different vulnerabilities. The game is available in both Chinese and English. The game claims to be an effective and fun way to learn security-related concepts; it also mimics a real-life problem environment in an orderly and transparent way and motivates players to learn more about security-related concepts. The game was evaluated and had positive results and said to be helpful for players to understand security attacks and vulnerabilities.

Cyber Detective (Lopes et al., 2018) is a 3D decision-making game that intends to teach cybersecurity awareness. The game was created using the Unity 3D game engine and will be able to be deployed to different environments. The player must complete an assortment of mini-games about sharing data in social networks, phishing, and the significance of creating strong passwords. After the mini-game, each of the player's decisions is explained and whether or not the answers are correct or incorrect. This keeps the player literate of the different situations that can happen based on their behavior/decisions using the web. The test product was created for mobile devices, and some initial tests were executed with teenagers. The

tests displayed that teenagers significantly refined their cybersecurity proficiency after playing the game.

Google's *Interland* (Seale & Schoenberger, 2018) is a 3D game that aims to help students to be safe and successful citizens in our networked world. The primary audiences for this game are second- to sixth-grade children. The concepts taught are anti-bullying, strong passwords, being careful what you post online, and phishing detection. Some mini-games make learning the concept interactive and fun. This game awards students a certificate after completion of the game.

Attacker-Centric Gamified Approach (Adams & Makramalla, 2015) is an approach that intends to teach all workers and organizational leaders to create cybersecurity skills and better protect and respond to data breaches. The approach was created by evaluating the following literature topics: gamification, cyber attackers and their attributes, and entrepreneurial view. In the approach, eight attacker types were chosen utilizing their motivation, knowledge/skills, and resources as attacker characteristics. Additionally, six entrepreneurial views were used to emphasize their motivation, knowledge/skills, and resources. The attacker types and their characteristics were united with the entrepreneurial views to create avatars for the game. The story is created using avatars' attacker type and characteristics. This approach allows newcomers to confront an attack via the lens of a cyber attacker and from entrepreneurial views. The approach has not been tested.

Internet Hero (Kayali et al., 2014) is a game that intends to teach children ages nine to twelve the technical and social basis of how to use the Internet. In the game, the player has to complete various mini-games aligned to four features of Internet use: emails, malicious programs, social networks, and connection types. To solve the games, players must comprehend the fundamental technical or civil aspects of these topics. To raise the personal interest of users, researchers depended on recognition with characters in the game and established a public context through play in class and shared leaderboard. A group of 50 children—25 boys and 25 girls—tested the game. The results enable researchers to update the game.

Games That Teach Anti-Phishing

What.Hack (Wen et al., 2019) is a decision-making game that aims to teach students anti-phishing methods by recreating some of the scenarios that people usually encounter. It captivates players by giving them the right to test and discover narrative outcomes, and delivers a set of learning subject matter through an exercise advancement that starts slow and moderately grows more complex. It was built with the Unity 3D game engine. The game focuses on three popular phishing topics: similar domain attack, URL manipulation, and malicious attachment. The game was apt to enhance players' precision in pinpointing upcoming threats by 36.7%,

even though a different game played by a control group did not attain a significant improvement.

Bird's Life (Weanquoi, 2018) is a 2D decision-making game that aims to teach college-level students, as well as general concern individuals, about Anti-phishing. It was built with the Unity 3D game engine. Players will make progress to gain knowledge in phishing attacks and how to steer clear of them in real-world scenarios through an enjoyable gaming environment. The game can be released to various platforms such as PC, web, and mobile devices. A pre-test, post-test, and online survey were established and used in the assessment process to calculate the results of this game. The pre-test and post-test contrast of 100 students displayed that the game had an effective impact on students' learning about phishing attacks.

Anti-Phishing Educational Game (Arachchilage & Hameed, 2017) is a game that aims to combine people's "self-efficacy" into game design to educate themselves on preventing phishing attacks. The game teaches how users can recognize legitimate URLs (Uniform Resource Locators) from fraudulent ones. This concept is based on the thought that a game can provide anti-phishing education, but can also provide a better learning condition because they can provide immediate feedback to motivate users. The proposed game should enhance the individual's phishing threat avoidance behavior.

Security Concepts with Alternate Reality Games (ARG) (Flushman et al., 2015) is a game that aims to teach security concepts to undergraduate students. The setting was a course that taught computer science core principles, exploring concepts through the lens of cybersecurity. This approach allowed users from any level of computer science to be engaged, which allowed for inclusiveness and support to new computer science students. The researchers assessed the student level to put them in the appropriate group with a similar learning level.

Games That Teach **Device Security** and Privacy

Be Aware! (Sharma et al., 2019) is an augmented reality game that intends to teach about compromised ATMs. The game was developed for the Android OS. The game was built using the Unity 3D game engine, ARcore Platform, Visual Studio, and Blender. The gameplay goes as follows: 3D models of two compromised ATMs are displayed together with an uncompromised ATM. With the assistance of Augmented Reality, the user has to pinpoint the machine that is not compromised by physically moving the smartphone to discover and distinguish the compromised parts of the ATM. The game is making users aware of a scam called ATM Skimming and Credit Card Skimming. ATM Skimming is when scammers use a camera and skimming device to steal the victim's credit card details. Card Skimming is when the attacker uses a device to steal the victim's credit card information from a regular transaction. The game has not been evaluated.

What Can Go Wrong? (Zargham et al., 2019) is a decision-making game that aims to raise awareness of general privacy and security concerns on mobile devices. This game is made for the desktop and incorporates humor as a tool to build motivation. The game covers the topics of screen-locks, phishing attacks, malicious Android Packages (APKs), and app permissions. A group of 21 participants evaluated the game and claimed the approach was successful in captivating and raising awareness. This study introduced a point that incorporating humor into the process can motivate users to learn.

(Smart)Watch Out! (Williams et al., 2019) is an online simulation that aims to teach security and privacy on smartwatch devices. Researchers investigated if protective behavior could be inspired by the use of a smartwatch simulation or PC application. Participants completed privacy problems on a simulated interface, directly running through protective actions. The privacy challenges are questions that ask users about the settings of their smartwatch devices. To evaluate the influence of the game, researchers studied the concerns and behaviors of five hundred and four smartwatch owners. Pre-test and post-test questionnaires were given to measure the effect. The testing group was split into two groups: one-half of the users played the game (treatment group), while the other half did not (control group). The results from the questionnaires showed that the treatment group's protective behavior, such as configuring the setting on their devices, became significantly more frequent, and the control group did not vary in protective behavior throughout the study.

Make My Phone Secure! (Bahrini et al., 2019) is a gamified approach that intends to educate users about cell phone permission security. The approach was built using the Unity 3D game engine. The method uses three scenarios to cover cell permission security. First, in the "Instagram Hears My Conversations" scenario, the microphone feature of the application is requesting to be on; this permission may have the potential to send targeted advertising. Next, in the "Flashlight Could Steal My Data" scenario, the flashlight application is requesting to gain access to the user's storage. This permission may have the potential to steal user data. Finally, in the "Shoppingtogo Sends Spam Messages" scenario, the shopping application requests access to the user's contact information, to potentially sell contact information to a third-party vendor. A group of 20 people evaluated the process, and the findings concluded that the approach was fun and informative.

Secure Software Engineering

CounterMeasures (Jordan et al., 2011) is a single-player game that intends to teach about buffer overflows, scanning systems, and string format vulnerabilities. The game is executed using a Flash client. The client sends player commands to a Java

server, and the server executes commands and supplies game feedback via virtual machines. The evaluation had 20 participants, displaying efforts, learning, and engagement with the game in contrast to identical reading materials. The results indicate the game teaches computer security methods in half the time compared to reading.

Data-driven Security Game (DdSG) (Løvgren et al., 2019) is a single-player data-driven security game that intends to teach novice developers how to select conventional mitigation strategies and patterns to defend against different security attack scenarios. The game was built with the Unity 3D game engine with a database from Express Node.JS. The game automatically updates itself with new information from appropriate security-based online sources (e.g., Common Attack Pattern Enumeration Classification CAPEC). The game is targeted to help build secure software. Researchers assessed the game by allowing participants to play the game and leave comments. The findings show that the game would be able to assist participants in the training of mitigation strategies to defend versus attack scenarios.

Cryptography

Quasim (Vadla et al., 2018) is a gamified intelligent tutoring system (ITS) intended to teach quantum cryptography. The game is built using the Unreal 4 Engine 3D platform that has been upgraded to embed predefined instructional components comprising videos, audio dialogues, auto-graded quizzes, tests, and the database was SQLite. The system includes a dynamic import of media-rich instructional components from certified open source and social platforms to increase peer-peer learning. Sixty students were given problems to solve that were related to quantum cryptography. The students did a pre-survey and post-survey to test their knowledge before and after gameplay. The results were the scores of the students did increase in the study.

Cryptography 3D escape game (Deeb & Hickey, 2019) intends to teach students topics in Computer Security and Cryptography. The game was created using the Blender Game Engine version 2.79b. The game covered two security topics—Dumpster Diving and Caesar Cipher. The dumpster-diving scenario focused on teaching that sensitive information needs to be appropriately disposed of because it can be used for password cracking. The Caesar Cipher is used to teaching the basics of encryption and decryption in the game. In the game, you play as an avatar locked in a room, and you must solve the puzzles in the game to leave the room. The player must interact with the items in the room to find clues. A group of 16 students evaluated the game; they completed a pre-test and post-test about their experiences with the game. The results showed that the students successfully increased their knowledge of cryptographic concepts and that the students enjoyed the game.

Network and Web Security

The Security Protocol Game (Hamey, 2012) is a group activity that aims to help students understand the design and operation of protocols for secure data communications. The game explores security protocols and possible attacks against them. Utilizing pen and paper, envelopes, and printed game pieces, students can reproduce a range of computer network security protocols such as SSL and Pretty Good Privacy. A survey confirms that the game helps students understand the importance of the design, the function, and the attacks toward security protocols.

Internet security game by Next Generation Security (NGSEC) systems (Ariyapperuma & Minhas, 2005) is a game that intends to teach network security principles. The research explored the use of online security games as an educational tool for instructing network security in a pedagogical framework. The game has 11 levels; to obtain authentication credentials, users must solve each challenge. A web browser is utilized to retrieve the labs, and HTTP protocol is applied to transfer lab information across networks to clients. Students need to use login credentials for verification at the server. After finishing a level, the next challenge is sent by email. After the evaluation, researchers concluded that online labs increased students' understanding.

DDoS (distributed denial of service) attack (Johnson et al., 2018) is a 3D game that aims to help students comprehend what a DDoS attack is, what types are present and how they impact Internet users through visualization and gameplay. This game was made using the Unity 3D game engine and is self-contained; also, the game can be deployed to different platforms. Students start with the Network Components module, where they will learn the elements in the network, such as the functionality of routers, IP address, etc. Next, the Transmission Control Protocol (TCP) learning module helps students understand the purpose of the protocol and how it works with the Internet Protocol. The last module helps students learn about TCP SYN Flood, which is one type of DDoS attack. The game has the pre and post quizzes built-in with five multiple-choice questions built into the game, which allows students to reinforce the knowledge quickly.

SSETGami Secure Software Education Through Gamification (Suarez et al., 2017) is an approach that intends to instruct main concepts and skills on how to create secure web applications. The approach was developed using HTML5, which helps the application to be used in an online course. The topics covered in the game are SQL injection, broken authentication and session management, cross-site scripting, insecure direct object references, cross-site request forgery, missing

function level access, security misconfiguration, sensitive data exposure, unvalidated redirects and forwards, and using components with known vulnerabilities. Each topic has a module that is enclosed within a module background, trial module questions, and the predicted learning results of each module.

2. GAMES AVAILABLE ONLINE

The product survey was conducted through a search. The terms searched were "Cyber Security Games," "Firewall games," "SQL Injection," and "Cross-Site Scripting." Table 2 displays the 20 games found in the search the games were played and teaches different topics of cybersecurity. Although the volume of the games covers cybersecurity awareness, some games discovered were more technical. The topics ranged from cross-site scripting and SQL injection, among others.

This survey of cybersecurity games included more technical games. Tioh et al. (2017) and Hendrix et al. (2016) concluded that the bulk of the games were only dealing with cyber awareness. But in recent years, more games were developed for the more technical cyber audience. Some games had topics of Firewall concepts, SQL injections, and Cross-Site Scripting.

3. DISCUSSION

The literature survey revealed the advantages and disadvantages of serious games. This section presents the problems and successes of the various games. Hence, these facts can educate future developers or researchers. Table 3 shows the advantages and disadvantages.

The advantages of games start with their usefulness in teaching and engaging students in cybersecurity concepts, and that games can be updated to help with the relative content. Additionally, games are built with industry tools such as Unity 3D game engine, Unreal 4 game engine, and Buildbox.

The disadvantages of some games were the small testing groups questioned the validity of the game, and researchers are not able to configure the game to improve gameplay. Next, information overload and repeated information cause users to lose interest in the game. Next web-based applications can be an issue for users who do not have Internet access. Finally, lack of instructional components may cause users not to learn the topic.

Game Category	Game Name	Topic	Audience Level
Security Awareness	Cyber Awareness (U.S. Department of Defense, 2019a)	Sensitive Information – PII (personally identifiable information), PHI (personal health information), malicious code-phishing, compressed URLs, spear-phishing, leaked information	College and up
Network and Web Security	Cyber Challenge (U.S. Department of Defense, 2019b)	Firewall – where they should be placed on the network, Binary number operation, User's Intent – adversity thinking	College and up
Security Awareness	Growing an Online Reputation (Carnegie Mellon University, 2020)	Social Ethics – being able to conduct one's behavior on the Internet, Cyber Bullying – to point out abusing terminology against peers on the Internet.	K-12
Security Awareness	Proofpoint Security – Security Awareness Trial (Proofpoint, 2019)	Email Security, Phishing Attack, Spear Phishing Attack	College and up
Security Awareness	Aggie Life (Texas A&M Information Technology, 2019a)	Cyber Security Awareness (credit card usage and online purchase)	College and up
Security Awareness	Keep Tradition Secure (Texas A&M Information Technology, 2019d)	Cyber Security Awareness (credit card usage and online purchase), Phishing	College and up
Security Awareness	Football Fever: Secure Your Season (Texas A&M Information Technology, 2019c)	Cyber Security Awareness (credit card usage and online purchase), Phishing	College and up

Game Category	Game Name	Topic	Audience Level
Security Awareness	Fight Back (Texas A&M Information Technology, 2019b)	Cyber Security Awareness (credit card usage and online purchase), Phishing, User's Intent	College and up
Security Awareness	Cyber Security Lab (NOVA Labs, 2020)	Programming (coding challenge), Social Engineering, Password Cracking	6-12
Security Awareness	Interland (Google, 2019)	Anti-Bullying, Internet Safety, Phishing, Information Protection, Cyber Security Awareness	K-12
Security Awareness	Targeted Attack: The Game (Trend Micro, 2015)	Decision Making, Taking care of business and security cost, Adversity Thinking	College and up
Security Awareness	Anti-phishing Phil (Carnegie Mellon University, 2019)	Phishing Attack	6-12
Network and Web Security	Netsim (Atwater & Bocovich, 2019)	Network Security, Network Attacks	College and up
Security Awareness	Data Center Attack (Trend Micro, 2019)	Decision-making, Taking care of business cost and security cost, Adversity thinking, Management	College and up
Network and Web Security	Permission Impossible (Sehl, 2017)	Firewall concepts	College and up
Network and Web Security	Blue Team: The Game (Kuzmiak, 2017)	Firewall concepts	College and up
Network and Web Security	Google's XSS-Game (n.d.)	XSS Cross-Site Scripting	College and up

Game Category	Game Name	Topic	Audience Level
Network and Web Security	The Weakest Link: A User Security Game (n.d.)	Cyber Security Awareness (cybersecurity terms), Phishing	College and up
Network and Web Security	Injection Game (Hussain, n.d.)	SQL Injection, XSS Cross-Site Scripting	College and up
Security Awareness	Tomorrow's Internet (Center for Development of Security Excellence, n.d.)	Cyber Security Awareness (cybersecurity terms)	6-12

Table 2: Games Surveyed

CONCLUSION

In this paper, we surveyed serious games used for cybersecurity education and training. Many of these games teach cyber security awareness. Some of these games teach topics such as network and web security, cryptography, and secure software development. Some of these games target audiences of K-12 students, some are for college students, and some are for professionals in the cybersecurity workforce. We provide a catalog of available online games for teaching cybersecurity topics. This resource is helpful for instructors to select suitable games to use in teaching cybersecurity concepts.

ACKNOWLEDGMENT

This work is partially supported by NSF under the grant DUE-1821960 and 1821965. 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 NSF.

References

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review*, *5*(1), 5–14. https://timreview.ca/sites/default/files/article_PDF/AdamsMakramalla_TIMReview_January2015.pdf

Arachchilage, N. A. G., & Hameed, M. A. (2017). Integrating self-efficacy into a gamified approach to thwart phishing attacks. *arXiv preprint arXiv:1706.07748*. https://arxiv.org/pdf/1706.07748.pdf

Ariyapperuma, S., & Minhas, A. (2005, October). Internet security games as a pedagogic tool for teaching network security. In *Proceedings Frontiers in Education 35th Annual Conference* (pp. S2D-1). IEEE.

Atwater, E., & Bocovich, C. (2019). *CS4G Netsim.* https://netsim.erinn.io/

Bahrini, M., Volkmar, G., Schmutte, J., & Wenig, N. (2019, September). Make my Phone Secure!: Using gamification for mobile security settings. In *Proceedings of Mensch und Computer 2019* (pp. 299–308). ACM.

Bhardwaj, J. (2019). *Design of a game for cybersecurity awareness* (master's thesis, North Dakota State University). https://hdl.handle.net/10365/29758

Carnegie Mellon University. (2019). *Anti-phishing Phil.* https://www.ucl.ac.uk/cert/antiphishing/

Carnegie Mellon University. (2020). *Growing an Online Reputation.* http://www.carnegiecyberacademy.com/funStuff/onlineReputation/onlineRep.html

Center for Development of Security Excellence. (n.d.). *Tomorrow's Internet.* https://www.cdse.edu/multimedia/games/TomorrowsInternet/story_html5.html

Deeb, F. A., & Hickey, T. J. (2019). *Teaching introductory cryptography using a 3D escape-the-room game.* IEEE Frontiers in Education Conference (FIE) Covington, KY. https://doi.org/10.1109/FIE43999.2019.9028549

Flushman, T. R., Gondree, M., & Peterson, Z. N. J. (2015). 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)*.

Google. (2019). *Interland.* https://beinternetawesome.withgoogle.com/en_us/interland

Google's XSS-Game. (n.d.). https://xss-game.appspot.com/

Hamey, L. G. C. (2012, November). Using the security protocol game to teach computer network security. In *Proceedings of The Australian Conference on Science and Mathematics Education (formerly UniServe Science Conference)* (Vol. 9).

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game based cyber security training: Are serious games suitable for cyber security training? *International Journal of Serious Games*, *3*(1), 53–61. https://doi.org/10.17083/ijsg.v3i1.107

Hussain, J. (n.d.). *Cyber security game: Play injection attack game, SQL, XSS, injection web vulnerabilities.* https://injection.pythonanywhere.com/

Johnson, J., Weanquoi, P., Zhang, J., & Xu, J. (2018). Learn DDoS attacks with a game. In *Proceedings of the World Congress on Engineering and Computer Science* (Vol. 1).

Jordan, C., Knapp, M., Mitchell, D., Claypool, M., & Fisler, K. (2011, October). CounterMeasures: A game for teaching computer security. In *2011 10th Annual Workshop on Network and Systems Support for Games* (pp. 1-6). IEEE. https://doi.org/10.1109/NetGames.2011.6080983

Kayali, F., Wallner, G., Kriglstein, S., Bauer, G., Martinek, D., Hlavacs, H., . . . Wolfle, R. (2014, April). A case study of a learning game about the Internet. In *International Conference on Serious Games* (pp. 47–58). Springer, Cham.

Krause, M., Mogalle, M., Pohl, H., & Williams, J. (2015, March). A playful game changer: Fostering student retention in online education with social gamification. In *Proceedings of the Second (2015) ACM Conference on Learning @ Scale (L@S '15)* (pp. 95–102). Association for Computing Machinery. https://doi.org/10.1145/2724660.2724665

Kuzmiak, K. (2017, August). *Blue Team: The Game.* Unity 3D WebGL. https://groups.inf.ed.ac.uk/tulips/projects/1617/CharlesFirewallGameWebsite/Website/v0.7/index.html

Lopes, I., Morenets, Y., Inácio, P. R. M., & Silva, F. G. M. (2018). Cyber-detective—A game for cyber crime prevention. *Proceedings of Play2Learn 2018*, 175–191.

Løvgren, D. E. H., Li, J., & Oyetoyan, T. D. (2019, May). A data-driven security game to facilitate information security education. In *Proceedings of the 41st International Conference on Software Engineering: Companion Proceedings* (pp. 256–257). IEEE Press.

NOVA Labs. (2020). *Cybersecurity lab.* https://www.pbs.org/wgbh/nova/labs/lab/cyber

Proofpoint. (2019). *Awareness material: Try our security awareness training.* https://www.proofpoint.com/us/resources/try-security-awareness-training

Seale, J., & Schoenberger, N. (2018). Be Internet awesome: A critical analysis of Google's child-focused Internet safety program. *Emerging Library & Information Perspectives, 1*, 34–58. https://doi.org/10.5206/elip.v1i1.366

Sehl, S. (2017). *Permission Impossible.* Unity 3D WebGL. https://groups.inf.ed.ac.uk/tulips projects/1617/PermissionImpossible/

Sharma, A., Palrecha, D., & Parekh, M. (2019, March 15). Security awareness game (Augmented Reality). In *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur - India, February 26-28, 2019.* http://dx.doi.org/10.2139/ssrn.3353135

Suarez, H., Kincannon, H., & Yang, L. (2017). SSETGami: Secure software education through gamification. *KSU Proceedings on Cybersecurity Education, Research and Practice, 1*. https://digitalcommons.kennesaw.edu/ccerp/2017/education/1

Texas A&M Information Technology. (2019a). *Aggie Life.* (2019a). https://it.tamu.edu/aggielife/

Texas A&M Information Technology. (2019b). *Fight Back.* https://fightback.tamu.edu/

Texas A&M Information Technology. (2019c). *Football Fever: Secure Your Season.* https://footballfever.tamu.edu/

Texas A&M Information Technology. (2019d). *Keep Tradition Secure.* https://keeptraditionsecure.tamu.edu/

The Weakest Link: A User Security Game. (n.d.). https://www.isdecisions.com/user-security-awareness-game/

Tioh, J. N., Mina, M., & Jacobson, D. W. (2017, October). Cybersecurity training: A survey of serious games in cybersecurity. In *2017 IEEE Frontiers in Education Conference (FIE)* (pp. 1–5). IEEE.

Trend Micro. (2015). *Targeted Attack: The Game.* http://targetedattacks.trendmicro.com/

Trend Micro. (2019). *Data Center Attack: The Game.* http://datacenterattacks.trendmicro.com/

U.S. Department of Defense. (2019a). *Cyber awareness challenge 2020.* https://dl.dod.cyber.mil/wp-content/uploads/trn/online/cyber-awareness-challenge/launchPage.htm

U.S. Department of Defense. (2019b). *Cyber challenge.* https://www.cybermission.tech/#!/game/strike/1/intro

Vadla, S., Parakh, A., Chundi, P., & Subramaniam, M. (2018, June). Quasim: A multi-dimensional quantum cryptography game for cyber security. In *22nd Colloquium for Information System Security Education*, June 2018.

Visoottiviseth , V., Sainont, R., Boonnak, T., & Thammakulkrajang, V. (2018, July). POMEGA: Security game for building security awareness. In *2018 Seventh ICT International Student Project Conference (ICT-ISPC)* (pp. 1-6). IEEE.

Weanquoi, P., Johnson, J., & Zhang, J. (2018). Using a game to improve phishing awareness. *Journal of Cybersecurity Education, Research and Practice, 2018*(2), Art. 2. https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss2/2

Wen, Z. A., Lin, Z., Chen, R., & Andersen, E. (2019, April). What.Hack: Engaging anti-phishing training through a role-playing phishing simulation game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Paper 108, pp. 1–12). ACM.

Williams, M., Nurse, J. R. C., & Creese, S. (2019). (Smart) Watch Out! Encouraging privacy-protective behavior through interactive games. *International Journal of Human-Computer Studies, 132*, 121–137. https://doi.org/10.1016/j.ijhcs.2019.07.012

Yasin, A., Liu, L., Li, T., Wang, J., & Zowghi, D. (2018). Design and preliminary evaluation of a cyber security requirements education game (SREG). *Information and Software Technology, 95*, 179–200. https://doi.org/10.1016/j.infsof.2017.12.002

Zargham, N., Bahrini, M., Volkmar, G., Wenig, D., Sohr, K., & Malaka, R. (2019, October). What could go wrong?: Raising mobile privacy and security awareness through a decision-making game. In *Extended abstracts of the annual symposium on computer-human interaction in play companion extended abstracts* (pp. 805–812). ACM.