PROMOTING CYBERSECURITY AWARENESS UTILIZING A “BUILD YOUR OWN ADVENTURE” SERIOUS GAME

Christo Croucamp, Günther Richard Drevin and Dirk Snyman
School of Computer Science and Information Systems, North-West University, 11 Hoffman Street, Potchefstroom, South Africa

ABSTRACT

Cybersecurity is of critical importance as we continue into the digital era. With technology improving rapidly and the accessibility of such technological devices becoming more prominent globally, the need for proper cybersecurity awareness has drastically increased. This has led to a need for methods to improve cybersecurity awareness. This paper addresses one such method, a “build your own adventure” serious game, where the aspects of cybersecurity awareness are combined with effective gaming principles. A serious game that teaches the users about cybersecurity awareness in a novel way is proposed.

KEYWORDS

Cybersecurity Awareness, Serious Game, Build Your Own Adventure

1. INTRODUCTION

Technological advancement is happening rapidly, and with that, accessibility to devices. Globally, there are estimated to be around 5.31 billion cellular connections. Approximately 4.95 billion internet users, or 62.5 percent of the total population at the start of 2022, have access to the internet (Kemp, 2022). The need for adequate education regarding the internet, cyberspace, and cybersecurity is critically important. In organizations, the employee is one of the biggest threats to information security (Whitman and Mattord, 2022). With rapidly rising cyber-threats associated with the increase of accessibility to devices able to connect to the internet, the user’s lack of skills in protecting themselves is a serious vulnerability (Kshetri, 2019).

The high rate of growth in technology and the ease of connecting to the internet, social media, online communications, and the internet of things has led to most people being connected to cyberspace (Allers *et al.*, 2021). With people being connected to cyberspace without realizing it, the threat of unintentionally sharing personal information that can be used in an attack targeted at the user is always present. This vulnerability has led to cybersecurity becoming a necessary aspect relevant to all internet users. To achieve personalized data protection, the users need to be educated on safe practices that provide a solid foundation. Therefore, education on cybersecurity should become a critical component in the education of young people (AlShabibi and Al-Suqri, 2021). Recently, serious games (i.e., games with the intention to teach) have been proposed as a viable method of teaching cybersecurity (Allers *et al.*, 2021). Therefore, the aim of this paper is to expand on this idea and propose a serious game for promoting cybersecurity awareness among the youth.

2. THREATS OF CYBERSPACE

With cyberspace being a vast virtual environment, the threat of malicious entities using this platform to perform malicious actions on unsuspecting persons is growing daily. In this section the aim is to provide a cursory overview on the most common threats found in cyberspace, and how these threats function.

2.1 Types of Threats

Cyber threats are mostly experienced as an attack that is initiated by another human. This section will review different types of attack vectors that are commonly used. Although that natural threats also exist, these are not relevant to the study as they occur in the physical world and are therefore not discussed here. Table 1 categorizes the different threats related to cybersecurity.

Table 1. Twelve categories of threats to information security (Whitman and Mattord, 2022)

Category of Threat	Attack Examples
Compromises to intellectual property	Piracy, copyright infringement
Deviation in quality of service	Internet and power outages
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, lightning
Human Error or failure	Accidents, employee mistakes
Information extortion	Blackmail, information disclosure
Sabotage or vandalism	Destruction of systems or information
Technical hardware failures or errors	Equipment failures
Technical software failure or errors	Bugs, code problems, unknown loopholes
Software attacks	Viruses, worms, macros, denial of service
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

2.2 Types of Attacks

The nature of cyberspace creates opportunities for malicious entities to execute attacks on assets without leaving the comfort of home or their workspace. With the ease of executing these attacks becoming increasingly accessible and how the global state of things in 2020 to 2022 is, the number of cybercrimes has increased (Vojinovic, 2022). One of the core defence strategies against any form of cyber-attack is having knowledge about the types of attacks, how they are executed and what kind of danger these attacks pose (Allers *et al.*, 2021). Some of these possible attacks include:

Privacy Attacks: These attacks are designed to compromise data privacy and information on a system. These attacks are considered passive in nature because privacy attacks do not attempt to inflict any damage to a system or to compromise the integrity of the system. This form of attack hides in the system and gathers information anonymously (Padmavathi and Shanmugapriya, 2009).

Denial-of-Service attacks: With a denial-of-Service attack the attacker send a large number of connections or information requests to a target. The number of requests eventually becomes too much to handle not allowing the service to provide for the legitimate request. This could lead to a server crash or just loosing functionality (Whitman and Mattord, 2022).

Back Door attacks : By using a known or newly discovered access gateway, malicious entities can access a system or network through a back door (Whitman and Mattord, 2022). These back doors are sometimes designed by programmers that need to access the system and then not removed when the software is shipped. These access gateways can be used to further infiltrate the system or place malicious software that perform actions on the system or network.

Malware Attacks : Malware or Malicious software is designed with the intent to be malicious. These intentions could be from affecting a browser pushing advertising to a full system infiltration and disruption (Whitman and Mattord, 2022).

Password Attacks: falls under the term espionage or trespassing as the malicious entity is trying to gain access to information that does not belong to them. Trying to reverse engineer or guess a password is often referred to as cracking and various methods are used to try and find a person password these are (Whitman and Mattord, 2022):

Phishing : This is a method or using various strategies to trick a user into disclosing sensitive information, compromising online accounts, compromising computer systems, and/or other personal or organizational information technology resources (Abroshan *et al.*, 2021). These are mainly executed using emails to catch users that are not fully aware of the danger.

These threats are just some of the common instances and there are daily updates to antivirus services that help with protecting people from these kinds of threats. By being aware of them a person can further protect themself.

3. CYBERSECURITY AWARENESS THROUGH SERIOUS GAMES

The process of creating awareness with regards to cybersecurity refers to any activities designed to focus on cybersecurity issues and inform an individual about these issues. (Allers *et al.*, 2021) An awareness program is designed to keep information security at the forefront of a user's mind. (Whitman and Mattord, 2022). If this is accomplished, users will be aware of any issues that might be encountered and if the users knows what is to be expected they can counteract the attempt by the malicious entities without further intervention. There are various methods used from posters to videos to class sessions that promote cybersecurity awareness (Whitman and Mattord, 2022). An important aspect of security awareness is that it should be simplistic but also address the correct dangers that are encountered by the users. An awareness campaign should be actively implemented to ensure that the information is always being revised and addressed as new issues arise (Whitman and Mattord, 2022). One way of providing structured material designed around cybersecurity is to incorporate the learning material into a serious game that provides a fun and interactive experience.

3.1 Serious Games

A serious game can be defined as:

> "[a] *computer application, for which the original intention is to combine with consistency, both serious (Serious) aspects such as non-exhaustive and non-exclusive, teaching, learning, communication or the information, with playful springs from the video game (Game).*" (Alvarez and Djaouti, 2011).

By incorporating an education aspect to a game, we can provide a fun learning experience where users can learn about threats when using devices with access to the internet. This game can provide a safe environment that allows for mistakes to be made and, in turn, encourages learning from the mistakes. The game should also contain aspects to make the user want to play it again. These include originality, replayability, surprise, and creative control (Kramer, 2000).

Another aspect of gaming that can be implemented into a serious game is to allow the user to choose how the adventure will unfold by giving the user choices that impact the gameplay and story. These scenarios could emulate real-life threats and will enable the user to experience these threats in a safe environment before encountering them in the real-world context. By incorporating interactive storytelling based on threats readily available on the internet, users can learn to reduce their online self-disclosure footprint (Dincelli and Chengalur-Smith, 2020). By including "build your own adventure" aspects into a serious game, it is possible to create a gaming experience that contributes to the goal of spreading awareness about cybersecurity among young people, while retaining enjoyability and replayability without reducing the impact of the learning material.

3.2 Characteristics of a "Build Your Own Adventure" Game

The artefact will be designed using a "build your own adventure" model where actions in the game will provide the player with choices that will alter the game and provide an experience based on the choices made. These choices can change the path taken through the story or affect the character's abilities. Figure 1 shows possible routes through a stage in the game until eventually reaching the stage's final boss.

Another aspect that can be implemented into the game to promote replayability and fun is a roguelike aspect. Roguelikes are dungeon-exploration games in randomly generated environments with randomly generated events and equipment to create a unique experience every time the game is played. (Harris, 2020). These randomly generated events can be designed to implement common cybersecurity vulnerabilities experienced; using this, the player can learn about how these events occur and how to counteract them when encountered on personal devices.

The user will start at the staging area indicated by the start node in Figure 1.

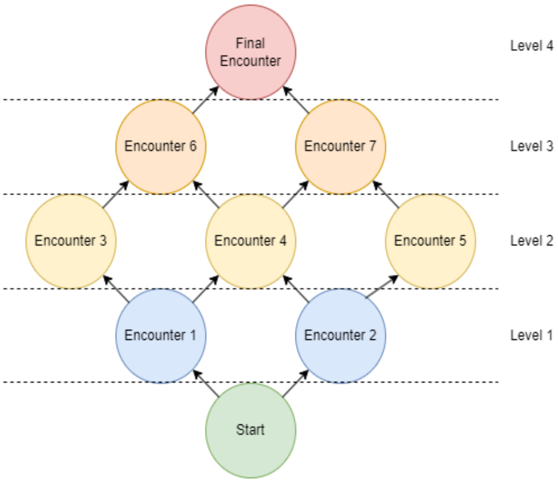


Figure 1. Possible paths of a character

This is where the user will make a choice on which character to play. Each character has their own strength and weaknesses. A choice on which room to progress to will also be made. This will then trigger the start of the adventure. Each room (node) will have a different event that occurs, and the difficulty of these events will scale with the level as indicated in Figure 1. This will create unique encounters as the user progresses through the stages, these unique encounters will also promote replayability will have to play the game multiple times to experience all the possible combinations of encounters.

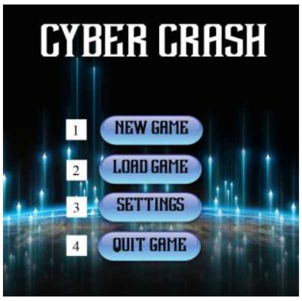


Figure 2. Start Menu

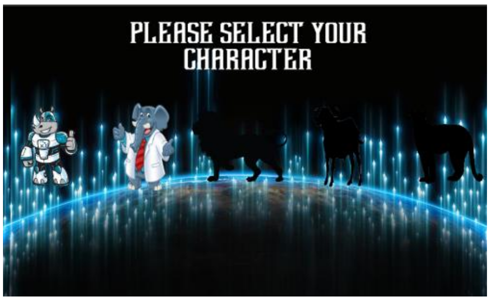
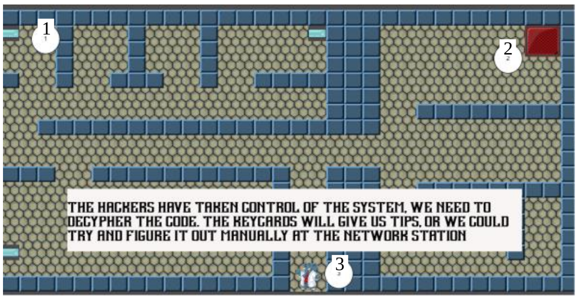

PLEASE SELECT YOUR CHARACTER

Figure 3. Character Select



THE HACKERS HAVE TAKEN CONTROL OF THE SYSTEM. WE NEED TO DECYPHER THE CODE. THE KEYCARDS WILL GIVE US TIPS, OR WE COULD TRY AND FIGURE IT OUT MANUALLY AT THE NETWORK STATION

Figure 4. Stage 1

4. CYBER CRASH GAME

The game will start like a normal game with a menu page as shown in Figure 2. This will serve as the gateway to the rest of the game. This screen consists of a background, a label that displays the games name, and four buttons that will navigate to separate sections of the game. *New Game* (1) leads to a new instance of the adventure, *Load Game* (2) leads to an already active instance of the adventure, *Settings* (3) allows the user to adjust game volume and other aspect of the game like difficulty and graphical adjustments. *Quit Game* (4) exits the program. Figure 3 shows the different characters and future characters than can be selected by the player, these characters each have different benefits, like the elephant having a larger memory capacity that can be used to store more information clues found in the adventure. This is the first choice made that affect the way the game will be played, and interesting characters will provide for a better experience. Figure 4 shows the layout of the first stage that implement a simple puzzle to decipher the system that has been infiltrated. This can be done in different ways by choosing to take the longer route and first go for the clue tokens (Figure 4 (1)) or go straight to the console and try to determine whether the system has been compromised (Figure 4 (2)). The goal is to finish the stage with the lowest number of actions possible. Allowing the user to choose the risk reward levels they are willing to take. Failed attempts at the cipher will lead to penalties being applied. That will affect the rest of the stages.

5. SUMMARY AND CONCLUSION

In this article, a youth-focussed cybersecurity awareness serious game, based on the characteristics of a "build your own adventure" approach, was proposed. This was achieved by identifying common cybersecurity threats and attacks and highlighting how serious games can be used to promote awareness of these threats. A brief overview of serious games, and how they can be developed to incorporate the principles of "build your own adventure" was presented. Finally, the resulting cybersecurity awareness game, *Cyber Crash*, was highlighted. By incorporating effective gaming strategies found in commercial games the goal of creating an effective cybersecurity game can be reached, by adding the "build your own adventure" aspect to promote better immersion when playing the game. By adding real world attack paths into the gaming environment, the user can learn about how malicious entities are attacking and learn how to counter these attacks.

REFERENCES

Abroshan, H., Devos, J., Poels, G. and Laermans, E. (2021), "COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic", *IEEE Access*, Vol. 9, pp. 121916-121929.

Allers, J., Drevin, G.R., Snyman, D.P., Kruger, H.A. and Drevin, L. (2021), "A mobile serious game to promote digital wellness among pre-school children".

Alshabibi, A. and Al-Suqri, M. (2021), "Cybersecurity Awareness and Its Impact on Protecting Children in Cyberspace", IEEE, pp. 1-6.

Alvarez, J. and Djaouti, D. (2011), "An introduction to Serious game Definitions and concepts", *Serious Games & Simulation for Risks Management,* Vol. 11, No. 1, pp. 11-15.

Dincelli, E. and Chengalur-Smith, I. (2020), "Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling", *European Journal of Information Systems,* Vol. 29, No. 6, pp. 669-687.

Harris, J. (2020), "Exploring Roguelike Games"*, CRC Press.*

Kemp, S. 2022. *Digital 2022: Global Overview report* [Online]. DATAREPORTAL. Available: https://datareportal.com/reports/digital-2022-global-overview-report [Accessed 10/05 2022].

Kramer, W. 2000. *What makes a game good* [Online]. The Games Journal, A Magazine about Boardgames. Available: http://www.thegamesjournal.com/articles/WhatMakesaGame.shtml [Accessed 01/05 2022].

Kshetri, N. (2019), "Cybercrime and Cybersecurity in Africa", *Journal of Global Information Technology Management,* Vol. 22, No. 2, pp. 77-81.

Padmavathi, D.G. and Shanmugapriya, M. (2009), "A survey of attacks, security mechanisms and challenges in wireless sensor networks", *arXiv preprint arXiv:0909.0576*.

Vojinovic, I. 2022. *More than 70 Cybercrime Statistics - A $6 Trillion Problem* [Online]. dataprot. Available: https://dataprot.net/statistics/cybercrime-statistics/ [Accessed 20/07 2022].

Whitman, M.E. and Mattord, H.J. (2022), "Principles of information security", *Cengage*.