

Cybersecurity Awareness on Personal Data Protection Using Game-Based Learning

Zamlina binti Abdullah*, Nurazian binti Mior Dahlan, Azlin binti Dahlan, Ahmad Faris Irfan bin,
Ahmad Samsul Arifin

Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Cawangan Melaka, Kampus
Jasin, Melaka, Malaysia

*zamlinaabdullah@uitm.edu.my, nurazian@uitm.edu.my, azlindah@uitm.edu.my, farissirfan2109@gmail.com

Abstract: The increasing digitalization in modern society has many positive effects on communication, business, education, banking and many more. Many individuals use their smartphones, tablets and laptops regularly and appear to believe the Internet to be a secure environment. However, it has also made people more vulnerable to a variety of cybersecurity risks. The rise in cyberattacks raises serious concerns about the lack of basic knowledge and awareness regarding cyber threats such as phishing, malware and password attacks. These cyber-threats can become dangerous for users as they can even cause identity theft and loss of money. The problem arises because lack of awareness of cybersecurity on personal data protection, a lack not a good understanding of how to protect the data, and a lack of knowledge to prevent cyber threats. Thus, this project proposes game-based learning to provide awareness and educate especially the youth on cybersecurity and personal data protection in a fun and effective way. The knowledge gained from the game can be applied to reduce the risks of cybercrimes. Agile methodology has been chosen for this project and has five phases which are requirement, design, development, testing, deployment and review. The enjoyment level of the game is evaluated by using an adaptation of the E-Game Flow Model including concentration, goal clarity, feedback, challenge, autonomy, immersion and knowledge improvement. Findings of enjoyment evaluation showed that the game receives an 82% level of agreeability by the game users. The game increases awareness among game users about cybersecurity. Future work for this game includes adding more levels into the game, covering other cyber threats and enhancing mobile devices.

Keywords: *Cybersecurity, cyber threats, enjoyment, game-based learning, agile methodology.*

1. Introduction

Since its emergence in the 1980s, the Internet has drastically changed the world (Wong et al., 2020). It has since become an integral part of people's daily lives, especially the younger generation as they are born into this new age of technology. Youngsters nowadays can access the Internet easily due to being fully equipped with various gadgets such as mobile telephones and smartphones (Abd Rahim et al., 2019). Cyber security is the activity of defending electronic systems, networks, computers, servers, mobile devices, data, and electronic systems against cyberattacks, theft, and destruction. It entails utilizing technology, procedures, and laws to safeguard systems and stop unauthorized individuals from accessing, using, disclosing, disrupting, altering, or destroying information (Cybersecurity and Infrastructure Security Agency, 2021). Many individuals believe the Internet to be a secure environment but numerous attacks happen every day (de Bruijn et al., 2017). With this rise of internet usage in education, cybersecurity education has become a must in both schools and universities. Every person who lacks cybersecurity awareness does so because they are unaware of the significance and consequences of cybersecurity (Rahman et al., 2020).

One of the causes of cyber threat problems among youth is a lack of knowledge of personal data protection (Abd Rahim et al., 2019). College students still do not have a good understanding of how to protect their data, even if they believe that they are being watched when using the Internet and that even university networks are not secure (Moallem, 2018). In addition, in a study by Kovačević et al. (2020), they found that students do not have enough awareness and knowledge of cybersecurity since no one was able to answer all the questions in the knowledge part of their questionnaire correctly.

The youth have no idea how to prevent cyber threats. They become more reliant on Internet technology for daily tasks, which has encouraged the expansion of the scope of participation in cyber-related activities. In contrast, the fundamental knowledge required for mitigating cyber risks is still lagging (Mai & Tick, 2021). Students lack the necessary comprehension and knowledge of the significance of information security principles and their practical applications (Moallem, 2019).

Based on the problems mentioned above, there is a necessity to boost awareness about cybersecurity among youths. This paper aims to present an enjoyable game-based learning application for youths to be concerned about the risks of cyber-related activities.

2. Literature Review

Cybersecurity awareness is the knowledge of, and application of, defenses against, online threats and vulnerabilities. It entails being conscious of potential risks, preventing those risks, and being prepared to respond in the case of a cyberattack. People must not only be aware of potential cyber hazards but also act properly, as is made clear by this statement (Bada, Sasse & Nurse, 2019).

In research by Garba et al. (2020) on student cybersecurity awareness, they discovered that although they had a high level of awareness in a few areas, including privacy and trust, the students lacked essential knowledge about password security, phishing, and two-factor authentication. Additionally, according to another study by Blancaflor et al. (2021) on students' vulnerability to malware, 63% of the devices examined for the investigation had malware installed on them or already existed on them.

A. Cyber Threats: Phishing is the practice of pretending to be a reliable entity in an electronic conversation to get sensitive data like usernames, passwords and credit card numbers (Bhavsar, Kadlak & Sharma, 2018). Passwords are the only security measure used to keep an application safe from unwanted access, but sadly, many users do not completely understand how important passwords are (Chanda, 2016). Malware is used to penetrate a computer system or network as part of a cyber-attack to disrupt operations or obtain access to the system's resources without authorization (Symantec, 2019).

B. Game-Based Learning (GBL): By incorporating entertainment into the learning process, GBL aims to increase student participation in learning while playing and to make learning more exciting (Al-Azawi, Al-Faliti & Al-Blushi, 2016). Since they are frequently introduced to students by professionals in charge of the teaching process, who direct students to play rather than the students beginning to play voluntarily or through recommendations from friends, player enjoyment is especially crucial for educational serious games (Ferreira de Almeida & dos Santos Machado, 2021).

C. Agile Methodology: Agile stands for moving quickly, which emphasizes iterative and incremental models in software development (McCormick, 2012). This methodology makes it easy for the developer to make modifications when developing the product. This method was created to make the most of the time and resources available for software design. Changes can be quickly included in the software product because it is built in small batches (McCormick, 2012). There are six phases consisting of requirements, design, development, testing, deployment and review.

D. E-Game Flow Model: The E-Game Flow model of player satisfaction is made up of 38 criteria taken from the literature on game user experiences and organized into eight components that conceptually correspond to Csikszentmihalyi's idea of flow (Sweetser, 2020). The eight core elements in the model are concentration, challenge, skills, control, clear goals, feedback, immersion, and social interaction. This study implements the E-Game Flow Model to evaluate the user's learning cognition of enjoyment while playing the game.

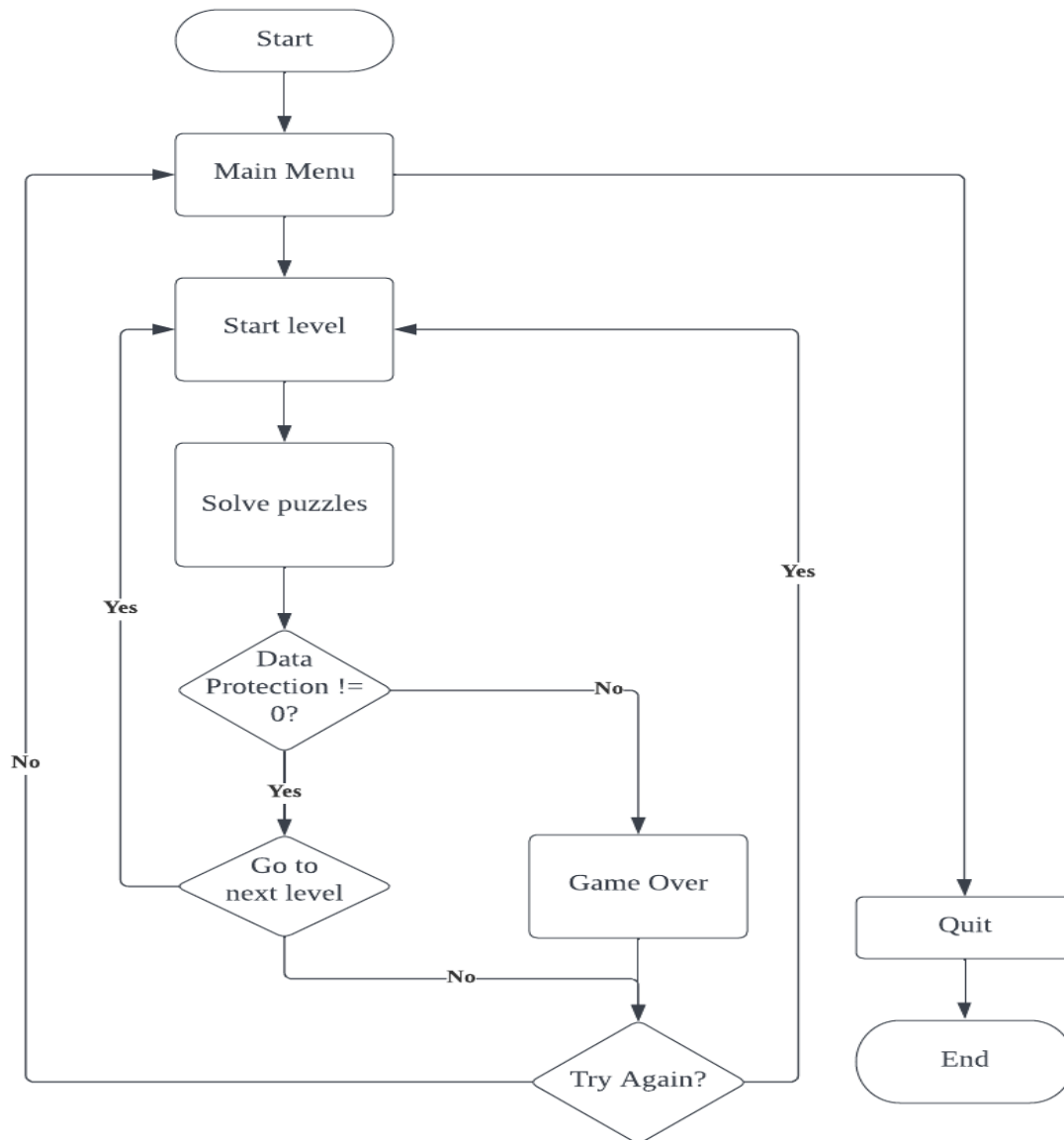
3. Methodology

The game's development is guided by the agile methodology that involves 6 phases which are requirements, design, development, testing, deployment and review.

A. Requirements: Many journals and articles were reviewed to get information about this topic, such as cybersecurity education, the implementation of game-based learning in education and several existing games about cybersecurity awareness. All the data gathered will be used to identify the problem and determine the objectives, scope and significance of developing this project.


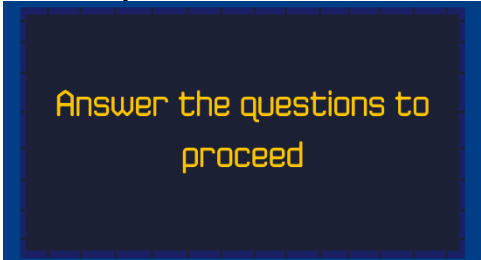




B. Design: The design phase is where the developer needs to design a flowchart and a storyboard before further development. Figure 1 shows the flow of the game.

Figure 1: Flow of the Game

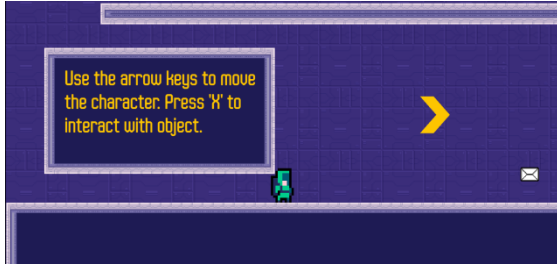


C. Development: The game is developed using the Construct 3 game engine and the designing tools are Piskel and Canva. Construct 3 is an HTML-based 2D video game engine to facilitate the rapid development of games through visual programming, easy to use and powerful. Construct 3 is a 2D video game engine that uses visual programming to make it easy for non-programmers to create games. Piskel is free and open-source pixel art software that can be used to create animations and sprites. Canva is an online graphic design platform that allows users to create a variety of visual content, such as posters, social media graphics, presentations, flyers and more. It is easy and user-friendly interface makes for both experienced and new users to utilize the platform. The project development involved the elements of the E-Game Flow model to enhance the enjoyment of users while playing the game. All the elements are highlighted and explained in detail in Table 1.

Table 1: Implementation of E-Game Flow Model in Cybersecurity Awareness

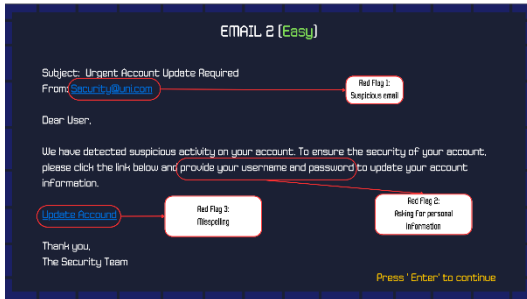
Elements	Criteria
<p>Concentration</p> 	<p>The straightforward gameplay makes the player stay focused and concentrate on the gameplay instead of being distracted by other things.</p>
<p>Goal Clarity</p>  	<p>Clear goals and hints are presented throughout the game to make sure players know the goals of the game.</p>
<p>Feedback</p> 	<p>The game provides feedback for the player's actions during most of the gameplay. For example, when the player chooses the wrong answer, a pop-up panel will appear saying that the player chooses the wrong answer, and a wrong sound will be played.</p>
<p>Challenge</p> 	<p>The game provides the player with adequate challenges that scale as the game progresses. As the game progresses, the question will be harder and the player will need to answer the questions to proceed.</p>
<p>Autonomy</p> 	<p>The game provides the player with the necessary information such as their remaining lives and hints for progressing through the game. The game also provides the player with the ability to pause</p>

Immersion



and stop the game whenever they want. To add a sense of immersion to the gameplay, feedback sounds and background music is added to the game to make the players feel more immersed.

Knowledge Improvement



The player will be able to gain knowledge on the topic of cybersecurity throughout the game by answering the questions and reading the explanations after answering.

D. Testing: Testing is conducted using an online questionnaire to 20 university students. The questionnaire is designed by the E-Game Flow model to measure the level of enjoyment and the effectiveness of the game. Seven factors have been highlighted in the questionnaire that are concentration, goal clarity, feedback, autonomy, challenge, immersion and knowledge improvement. The game and the form evaluation’s link have been distributed through Google Drive to the participants. Participants have 15 minutes to play the game before answering the questionnaire. The questionnaires are in Google Forms for participants to fill out and submit after testing the game.

E. Deployment: The Developer will deliver the product to the client once it is completed and present all the details of their requests and requirements (McCormick, 2012). In this phase, the game is ready to be published on the Internet and available for all people to play.

F. Review: Review is the final stage of the agile process. The developer receives feedback from the client and takes action to assess the project's progress considering the specified goal.

4. Results and Discussions

The enjoyment testing is analyzed based on the adapted seven dimensions of the E-Game Flow model. Table 2 is the summary of the analyzed information from the testing.

Table 2: Overall Total Mean Value

Factor	Total Mean
Concentration	4.18
Goal Clarity	4.26
Feedback	4.13
Challenge	4.04
Autonomy	4.20
Immersion	3.62
Knowledge Improvement	4.27
Total Average Mean	4.10

Table 2 indicates the mean value for each dimension and the overall mean of the seven dimensions. In the concentration dimension, the total mean is 4.18. This shows that participants strongly agree that they can remain focused on the game. The total mean for the goal clarity dimension is 4.26. Most of the participants strongly agree that they are clear with the game goals. The feedback dimension in this project is achieved with a total mean of 4.13. Most of the participants strongly agree that they receive feedback while playing the game. Next, the participants strongly agree with the challenge dimension in this game with the mean value is 4.04. The autonomy dimension is 4.20 which mean most of the participants strongly agree that the game provides a sense of control over the game. The mean for the immersion dimension is 3.62. The mean for knowledge improvement is 4.27. Participants strongly agree that they were focused, did not feel tired and forgot the time when playing this game. The overall average of the dimensions is 4.10 or 82%, which shows the participants strongly agree that the game is enjoyable and effective.

5. Conclusion

Game-based learning can be used to create an enjoyable learning experience and a more exciting environment. Learning through the cybersecurity game has been successfully designed and developed to help students get enjoyment while becoming aware of cybersecurity and cyber threats. The game helps students to have an enjoyable and interesting experience. Players also can learn about cybersecurity and cyber threats through the game content.

However, the project is developed for personal computers and Windows platforms only, with limited cyber threats scope, and a few levels are provided to show progress achievement. As a future work, it is highly recommended that enhancement to mobile platforms, include awareness of a variety of cyberthreats and add many levels to motivate players to learn with fun.

References

- Abd Rahim, N. H., Hamid, S. & Mat Kiah, M. L. (2019). Enhancement of Cybersecurity Awareness Program on Personal Data Protection among Youngsters in Malaysia: An Assessment. *Malaysian Journal of Computer Science*, 32(3), 221–245. <https://doi.org/10.22452/mjcs.vol32no3.4>
- Al-Azawi, R., Al-Faliti, F. & Al-Blushi, M. (2016). Educational gamification vs. game-based learning: Comparative study. *International journal of innovation, management and technology*, 7(4), 132-136.
- Bada, M., Sasse, A. M. & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behavior? arXiv preprint arXiv: 1901.02672.
- Bhavsar, V., Kadlak, A. & Sharma, S. (2018). Study on phishing attacks. *Int. J. Comput. Appl*, 182, 27-29.
- Blancaflor, E., Esguerra, C., Fandiño, C., Gonzales, A. L., Nisperos, B. & Pono, L. (2021, March). A. Assessment of Student Vulnerability on the Download of Malware Disguised as Cracked Software. In Proceedings of the 11th Annual International Conference on Industrial Engineering and Operations Management Singapore.
- Chanda, K. (2016). Password security: an analysis of password strengths and vulnerabilities. *International Journal of Computer Network and Information Security*, 8(7), 23.
- Cybersecurity and Infrastructure Security Agency. (2021). What is cybersecurity? Retrieved from <https://www.cisa.gov/what-cybersecurity>
- de Bruijn, H. & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), 1-7.
- Garba, A. A., Siraj, M. M., Othman, S. H. & Musa, M. A. (2020). A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach. *Int. J. Emerg. Technol*, 11(5), 41-49.
- Kovačević, A., Putnik, N. & Tošković, O. (2020). Factors related to cyber security behavior. *IEEE Access*, 8, 125140-125148.
- Mai, P. T. & Tick, A. (2021). Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytech. Hung*, 18, 67-89.
- McCormick, M. (2012). Waterfall vs. Agile methodology. *MPCS*, N/A, 3.

- Moallem, A. (2018, July). Cyber security awareness among college students. In International conference on applied human factors and ergonomics (pp. 79-87). Springer, Cham.
- Moallem, A. (2019). Cybersecurity Awareness among Students and Faculty. CRC Press.
- Rahman, N., Sairi, I., Zizi, N. A. M. & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, 10(5), 378-382.
- Sweetser, P. (2020, December). Game Flow 2020: 15 Years of a Model of Player Enjoyment. In 32nd Australian Conference on Human-Computer Interaction, 705-711.
- Symantec. (2019). What is Malware? Retrieved from <https://www.symantec.com/security-center/definition/malware>
- Wong, S. M., Leong, C. M. & Puah, C. H. (2020). Mobile Internet adoption in Malaysian suburbs: The moderating effect of gender. *Asian Journal of Business Research*, 9(3), 90-114.