Serious Games as a Strategy for Enhancing Filipino Cybersecurity Literacy and Interest

Christian Dale Encinares(crencinares@up.edu.ph)
Joshua Lloyd Doros(jsdoros1@up.edu.ph)

Computer Security Group (CSG)
Department of Computer Science
University of the Philippines Diliman

July 5, 2023

Abstract

The Philippines has seen an increase in the availability and usage of digital technologies such as the internet and mobile devices. Unfortunately, this technological development comes with the increased risk of cyber threats that can affect not just individuals, but also companies and organizations. The study aimed to create a digital serious game for the Windows desktop platform that tailored to the general Filipino population and provided them with information on basic cybersecurity principles and handling of common cyberattacks without the need for prior in-depth knowledge. The game consisted a series of arcade-style minigames that tackle best practices for internet safety, internet navigation, phishing attacks, social engineering. Through pre-test and post-test examinations of the players, the effectiveness of the game in raising cybersecurity literacy and interest was evaluated. The study's findings indicate that while playing the game positively influenced the players' interest in cybersecurity, it did not significantly impact their knowledge in the field.

Introduction

In recent years, the prevalence of cyber threats has increased, making cybersecurity a critical component of the Philippines' security posture. A significant amount of individual and organizational financial losses have been attributed to cybersecurity attacks including malware, hacking, and social engineering schemes[1][10]. This denotes the need to strengthen the cybersecurity literacy of the general public and also signifies the demand for cybersecurity professionals in our country. Despite the country's efforts to raise awareness and motivation in learning the preventive measures against threats in using digital technology, many still lack knowledge and interest in this field.

This paper developed a digital game-based learning tool with the aim of enhancing cybersecurity literacy and interest among the general Filipino public and aspiring cybersecurity professionals.

Background

With cyber threats looming around every corner and cybercriminals seeking to take advantage of their victims' vulnerabilities and weaknesses, be it lack of knowledge or training, there is a need for a more effective method of introducing cybersecurity literacy and awareness to the general public aside from traditional educational methods such as textbooks and lectures. Ideally, it should be a method that can attract and motivate students to learn more about cybersecurity and potentially even help them consider it as a career option. This is where serious games, as a method for education, come into play. With data from 2020 alone reporting that over 44 million of the country's population have played video games [5], serious games certainly presents itself as a possible medium for learning.

The term "Serious Games" sounds contradicting at first glance. After all, the word "Games" is usually associated with an activity that involves playfulness and entertainment while the addition of the word "Serious" implies otherwise. However, serious games have been defined as "any form of interactive computer-based game software for one or multiple players to be used on any platform and that has been developed with the intention to be more than entertainment" [8]. Following this definition, a good serious game must be able to strike a balance between its entertainment and practical aspects, in this case, education.

Serious games and the concept of gamification are often used interchangeably due to their relation with applied game elements, but these two are actually distinct. Gamification can be defined as "the use of game design elements in non-game contexts". The key difference between serious games and gamification is that gamification merely implements and adapts game elements (e.g. leaderboards and leveling systems) into something that isn't originally game related [4]. On the other hand, serious games utilize entire dedicated games, either digital or non-digital, as a catalyst towards a specific objective such as enhancing the learning experience by raising the student or player's engagement and interactivity.

Hendrix et al. reviewed and identified 28 cybersecurity training games with varying genres and topics covered ranging from cybersecurity awareness, network security, phishing, and end-user PC protection. They found that while these studies report a positive effect on their players, their sample sizes were small and only evaluated the short-term impacts on their game's players with some even having inadequate or even non-existent evaluations [7].

While there have been several previous applications of games for learning topics like Environmental Awareness and Waste Segregation[6], Philippine History [9], Philippine Geography [2], and Disaster Risk Reduction and Management in the Philippines [3], there is a notable scarcity and obscurity of initiatives for the topic of cybersecurity. Thus, this study aims to fill this gap in research by approaching cybersecurity learning in a way that is tailored to the local setting and experiences. In addition, the product's primary objective is to raise the general Filipino population's awareness and interest in the cybersecurity field and teach them the basic skills required to counter common cybersecurity attacks.

Methodology

Design Principle

The game design principles centered on the objective of creating an educational video game that strikes a balance between not requiring an extensive understanding of cybersecurity concepts and avoiding oversimplification. To achieve this, the implementation of simple controls, such as click and type was prioritized. This design choice allowed players to focus on comprehending the fundamental cybersecurity concepts rather than grappling with intricate game mechanics. The interactive and enjoyable nature of the game was realized through the incorporation of real-life scenarios and captivating gameplay variations. Additionally, a pastel color palette was deliberately selected to enhance the game's visual appeal, contributing to its immersive and engaging experience. Furthermore, the game's text elements are mostly composed in the Filipino language, with the aim of providing accessible cybersecurity education to Filipinos.

Storyboarding

The use of Canva was employed for the purpose of game screen storyboarding and conceptualization of user interface (UI) elements. Canva offered a diverse array of graphical components, effectively facilitating the visualization of the game screen. This choice was made to enhance the visual representation of the game, contributing to its overall design and aesthetic appeal.

Game Development

The Unity game engine (editor version 2021.3.17f1) was selected as the primary tool for game development. The decision to utilize Unity was driven by the accessibility and availability of game assets, as well as the abundance of online tutorials. The substantial user base of Unity proved advantageous, as it facilitated the swift acquisition of solutions through the active support of its community. The game was specifically designed for the Windows platform; however, Unity's compatibility with various other platforms, including iOS, Macs, and Android, allowed for potential future porting endeavors, thereby broadening its reach and accessibility.

The expeditious progress of the development process was achieved by implementing the Scrum framework, a widely recognized project management methodology. The researchers' familiarity with Scrum, owing to its prior inclusion in the department's software engineering course, informed its selection. To effectively manage Scrum, Notion was employed as a robust project management tool. Notion facilitated the seamless tracking of backlogs by employing its versatile database element, which could be visually represented as a table or board. Furthermore, important dates and relevant links were conveniently documented on a dedicated Notion page, ensuring efficient organization and management.

Playtesting and Survey

The playtesting process involved the distribution of a questionnaire to a sample of 37 participants. Snowball sampling was used to scout participants, preferring those with little to no background in cybersecurity. The questionnaire was designed to collect pertinent data regarding participants' general information, preliminary and post cybersecurity knowledge and interest, and specific feedback pertaining to different aspects of the game. The survey was administered in an unsupervised manner, allowing the respondent to answer the survey and play the game at their own pace.

Participants were requested to provide relevant personal details, including their name, email, contact number, age, gender (male, female, others), and nationality (Filipino, others). In addition, participants were asked to specify their occupation and educational background, indicating their respective school (e.g., UP Diliman). To further enhance the understanding of the participants' linguistic background, they were also prompted to indicate the languages they spoke and their preferred language. Two versions of the survey forms were also created, one in English and other in Filipino, to accommodate language preferences.

Before proceeding to the playtesting phase, participants were asked to share their level of interest and existing knowledge in the field of cybersecurity. The questionnaire featured a Likert scale, spanning from 1 to 5, with 1 representing “Strongly Disagree” and 5 representing “Strongly Agree.” This was used to gauge participants’ level of expertise, enthusiasm, inclination to seek information regarding cyber threats and protective measures, and overall confidence in cybersecurity-related endeavors. Furthermore, participants were assessed on their prior familiarity with specific cybersecurity scenarios through a set of multiple-choice questions that encompassed diverse aspects such as data breaches, password creation, and the handling of one-time pins (OTPs).

Upon the completion of the playtesting phase, participants were then prompted to offer their post-test responses, focusing on their continuing interest in cybersecurity. Similar statements to those presented in the pre-test section were provided.

The survey was also designed to solicit participants’ feedback regarding specific facets of the game. Participants were encouraged to rate various elements related to the game’s user interface (UI) and graphics, encompassing parameters such as intuitiveness, ease of navigation, and visual appeal. Furthermore, participants were invited to provide their insights on the responsiveness of game controls and the presence of any potential glitches or bugs encountered during gameplay. Participants were encouraged to report any observed issues. Additionally, participants were requested to offer feedback on their sense of achievement derived from successful game completions and their perception of the game’s replayability.

The survey dedicated a section that allowed participants to express any additional comments or suggestions pertinent to their gameplay experiences.

Statistical Analysis

The study employed right-tailed paired samples t-test to compare participants’ pre-test and post-test responses, evaluating if there are significant differences in their cybersecurity awareness scores before and after the playtesting phase. Two samples independent t-test was also employed to compare pre-test and post-test responses for participants who are Computer Science undergraduates and non-Computer Science undergraduates.

Results and Discussion

Cyberscapes

A cybersecurity game, Cyberscapes, was produced. This game can be downloaded and installed on Windows desktop computers. It comprises a collection of arcade-style minigames designed to address various general cybersecurity concepts, with a specific emphasis on social engineering techniques and fundamental practices for threat prevention.

The game was hosted on itch.io to allow the participants of the study to play remotely via their browser. They were also provided the option to download and install the game locally. By engaging in these minigames, participants were equipped with knowledge and skills to mitigate potential cybersecurity threats encountered in their day-to-day activities. The subsequent subsections provide a comprehensive description of the game screens and mechanics employed in the cybersecurity game.

Welcome Screen

Upon launching the game, the player was first presented with the welcome screen. This screen contained a play button to begin playing the mini-games, a credits section that provided information about the people involved in the game's creation, and a quit button that allowed the player to exit the game when desired.

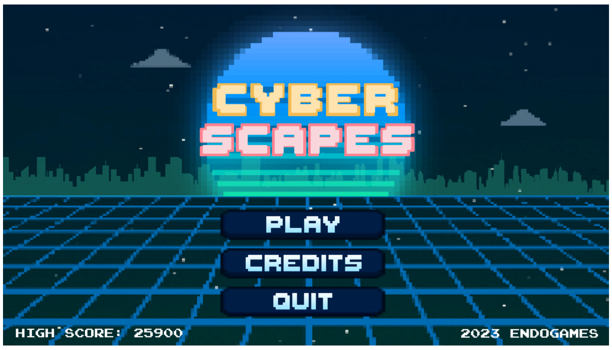
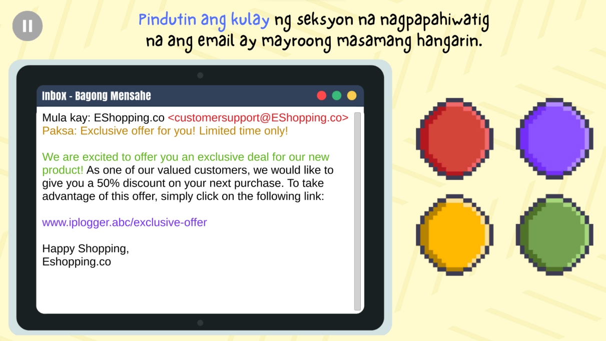


Figure 1: The Welcome (Main Menu) Screen

[MG-01] Email Red Flags

The objective of this mini-game was to educate the player on tactics for combating email-based phishing attacks. This was achieved by having the player inspect a scam email. The player's task was to select the correct color-coded section of the email that best explained why the email was likely to be malicious using the four available buttons.



Pindutin ang kulay ng seksyon na nagpapahiwatig na ang email ay mayroong masamang hangarin.

Inbox - Bagong Mensahe

Mula kay: EShopping.co <customersupport@EShopping.co>
Paksa: Exclusive offer for you! Limited time only!

We are excited to offer you an exclusive deal for our new product! As one of our valued customers, we would like to give you a 50% discount on your next purchase. To take advantage of this offer, simply click on the following link:

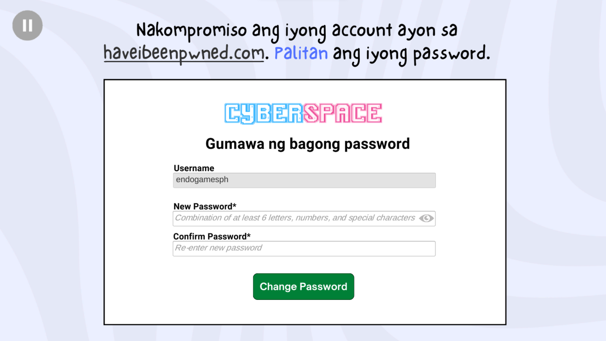
www.iplogger.abc/exclusive-offer

Happy Shopping,
Eshopping.co

Figure 2: An instance of MG-01

[MG-02] Create a Strong Password

Two variants were offered by this minigame. The first variant was designed to motivate players to regularly update their passwords, especially after a significant data breach. Players were tasked with typing a new password that met specific criteria, including the use of special characters, capital letters, and numbers. The challenge was to create a password that satisfied the required criteria in order to progress to the next level.



Nakompromiso ang iyong account ayon sa haveibeenpwned.com. Palitan ang iyong password.

Gumawa ng bagong password

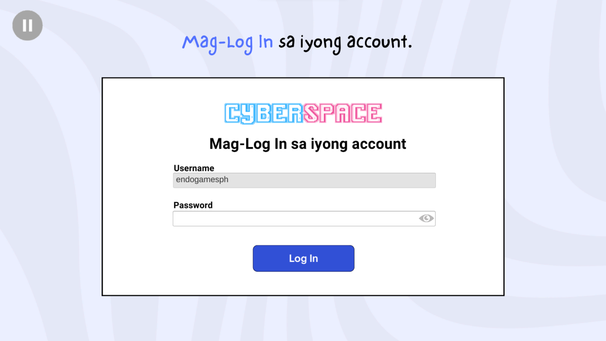
Username
endogamesph

New Password*
Combination of at least 6 letters, numbers, and special characters

Confirm Password*
Re-enter new password

Figure 3: An instance of MG-02.1

The second variant was focused on enhancing players' ability to remember their passwords. In this variant, the credentials set in the previous variant had to be utilized by the players to successfully log in. This tested their memory in recalling the correct password.



Mag-Log In sa iyong account.

Mag-Log In sa iyong account

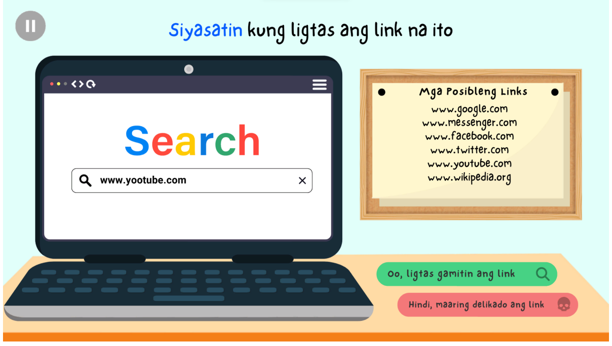
Username
endogamesph

Password

Figure 4: An instance of MG-02.2

[MG-03] Only Enter Trusted Sites

The objective of this mini-game was to instill the habit of inspecting and double-checking URLs and hyperlinks for possible typographical errors in order to protect individuals from falling victim to phishing and typosquatting. The player had to assess whether the provided link was safe to proceed with or the link is possibly deceptive.



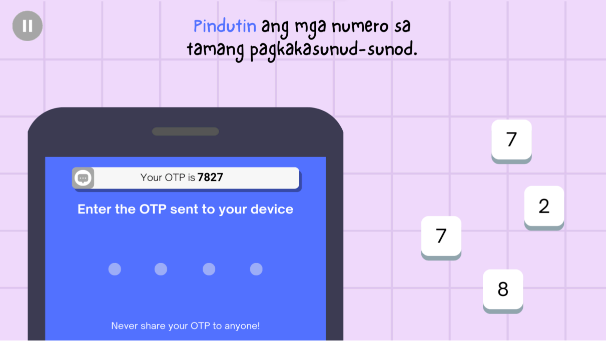
Siyasatin kung ligtas ang link na ito

Mga Posibleng Links
www.google.com
www.messenger.com
www.facebook.com
www.twitter.com
www.youtube.com
www.wikipedia.org

Figure 5: An instance of MG-03

[MG-04] Two-Factor Authentication

This mini-game had two purposes: to educate the player about the usage of one-time passwords (OTPs) and to reinforce the importance of not sharing OTPs with others. Players had to correctly arrange a sequence of numbers that corresponds to the given code.



Pindutin ang mga numero sa tamang pagkakasunud-sunod.

Your OTP is **7827**

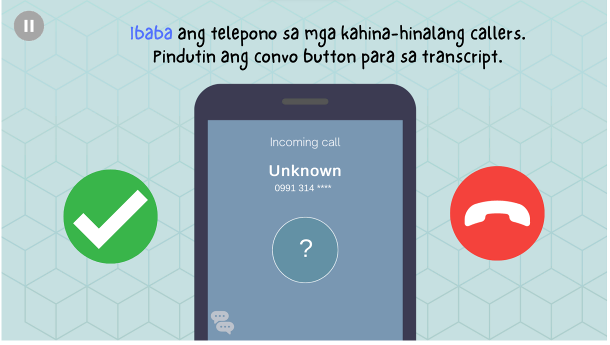
Enter the OTP sent to your device

Never share your OTP to anyone!

Figure 6: An instance of MG-04

[MG-05] Hang Up on Scammers

In this mini-game, players were presented with a phone conversation and were challenged to discern whether the call was authentic or deceptive. By carefully analyzing the conversation's content and context, players had to make a judgment call and determine the caller's true intentions.

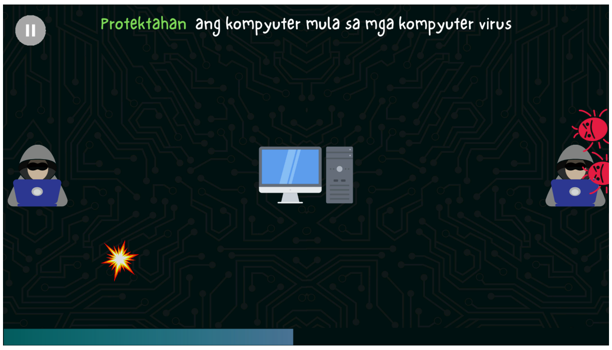


Ibaba ang telepono sa mga kahina-hinalang callers.
Pindutin ang convo button para sa transcript.

Figure 7: An instance of MG-05

[MG-06] Turn on your Antivirus

The goal of this mini-game was to serve as a reminder for the player to always have their computer's anti-virus protection enabled in order to safeguard themselves against the potential risks posed by viruses and malware attempting to infiltrate their computer. The player's task was to protect the desktop located at the center of the screen by "squishing" the viruses that tried to approach it.

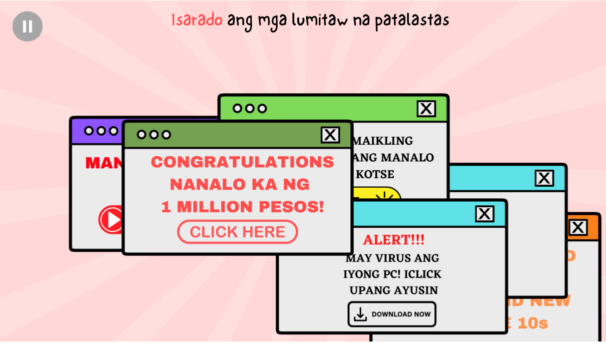


Protektahan ang kompyuter mula sa mga kompyuter virus

Figure 8: An instance of MG-06

[MG-07] Close the Popup ads

The objective of this mini-game was to educate the player about the importance of not clicking on pop-up advertisements that appear on their screen, as doing so could potentially redirect them to suspicious websites. Instead, the player must learn to either ignore the ad or close the pop-up window. In the mini-game, players were specifically challenged to exit the advertisement without clicking on the window itself.



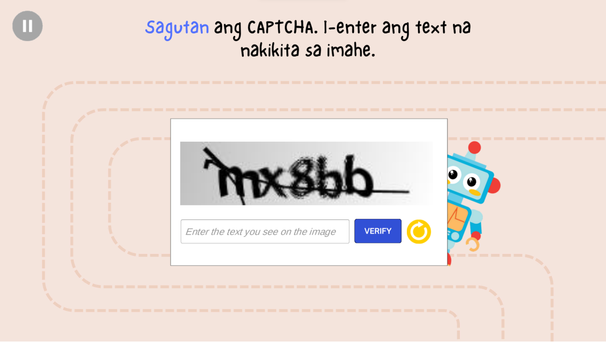
Isarado ang mga lumitaw na patalastas

Figure 9: An instance of MG-07

[MG-08] Accomplishing CAPTCHAs

Through this minigame, players were provided with insights into the role of CAPTCHAs in safeguarding web servers from automated bot attacks. The game featured two variants: the Gimpy Text CAPTCHA form and the Google Image reCAPTCHA form.

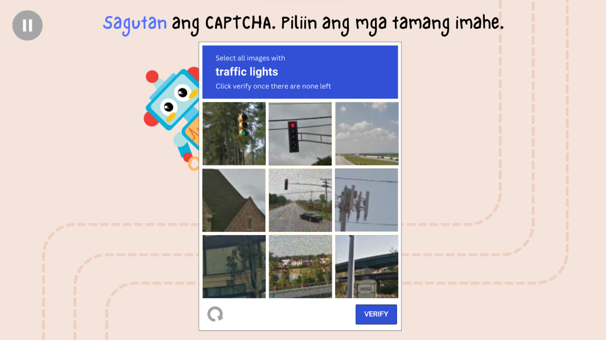
In the first variant, players were presented with distorted or warped images and were tasked with entering the corresponding text they observed. This exercise aimed to improve their ability to accurately transcribe the text, highlighting the effectiveness of text-based CAPTCHAs.



Sagutan ang CAPTCHA. I-enter ang text na nakikita sa imahe.

Figure 10: An instance of MG-08.1

The second variant was focused on the Google Image reCAPTCHA form, where players were required to select the images that aligned with the provided instruction from a group of nine images.



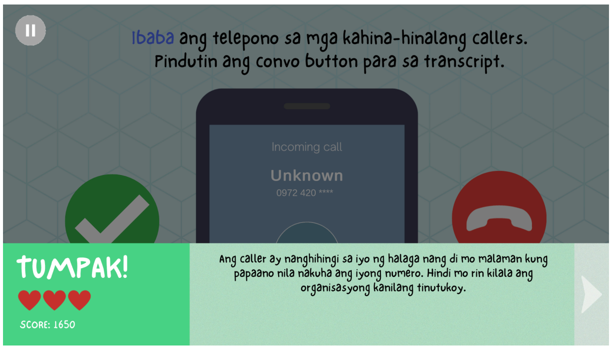
Sagutan ang CAPTCHA. Piliin ang mga tamang imahe.

Select all images with
traffic lights
Click verify once there are none left

Figure 11: An instance of MG-08.2

Post-Minigame Prompt

A panel popped up whenever the player finished a minigame, regardless of meeting the winning or losing condition. The user's current score, remaining lives, and concepts pertinent to the topic the mini-game was tackling are displayed on this panel.



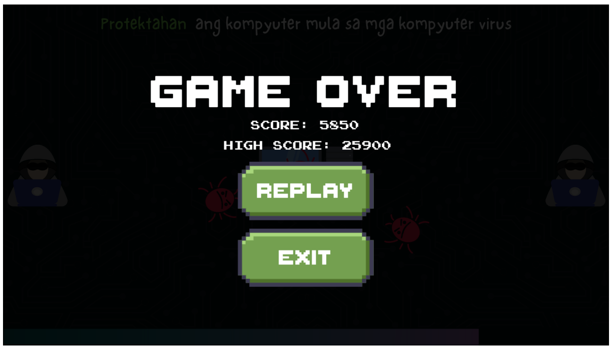
Ibaba ang telepono sa mga kahina-hinalang callers. Pindutin ang convo button para sa transcript.

Ang caller ay nanghihingi sa iyo ng halaga nang di mo malaman kung papaano nila nakuha ang iyong numero. Hindi mo rin kilala ang organisasyong kanilang tinutukoy.

Figure 12: A screen showing the current score, remaining lives, prompt message

Game Over

After all three lives were exhausted, players were directed to a game over screen where their final score and high score were displayed. At this point, players were given the option to either return to the main menu or initiate another round of the game.



Protektahan ang kompyuter mula sa mga kompyuter virus

Figure 13: A screen showing a Game Over message

Enhancing Cybersecurity Literacy and Interest

The researchers conducted a survey to assess the cybersecurity knowledge and interest of the participants before and after playing the game. A total of 37 respondents took part in the survey and playtesting. A right-tailed paired samples t-test performed on both the pre-test and post-test cybersecurity interest cumulative scores yielded a p-value of approximately 1.277×10^{-5} which is less than the significance level of 0.05. This indicated that the game was able to raise the players' interest in cybersecurity. Performing the same test on the pre-test and post-test cybersecurity knowledge however, yielded a p-value of approximately 0.305 which is greater than the significance level, 0.05. This implied that there was no significant difference between the average pre-test score and the average post-test score with regards to the participants' cybersecurity knowledge, indicating that the game did not enhance their knowledge.

Among the 37 respondents, 11 individuals are either currently pursuing or currently possesses a degree in BS Computer Science. A two samples independent t-test performed between the cybersecurity interest of respondents who are Computer Science undergraduates versus Non-Computer Science undergraduates revealed a p-value of approximately 0.892 which is greater than the significance level of 0.05. This meant that the average improvement of cybersecurity interest between the two were almost equal. In a similar fashion, a two samples independent t-test was also performed on the prior cybersecurity knowledge and interest between Computer Science undergraduates and non-Computer Science undergraduates which resulted with p-values of approximately 0.197 and 0.346 respectively. This indicates that the cybersecurity knowledge and interest between Computer Science undergraduates and non-Computer Science undergraduates were already on par with each other prior to playing the game.

Gameplay Experience

In the survey, the playtesters were asked to rate their experiences with playing the game, particularly with regards to its UI/Graphics, Responsiveness and Ease of Gameplay, Sense of Achievement, and Replayability.

Statement	Rating
Intuitiveness	4.567568
Navigation	4.729730
Graphics	4.675676
Difficulty	4.594595
Responsiveness	4.729730
Glitches/Bugs	4.756757
Completion Pride	4.486486
High Score Pride	4.621622
Playing Again	4.405405
Game Variation	4.135135
Non-Repetitive	3.972973

Table 1: Average Ratings for Cyberscapes' Gameplay Experience.

The game's replayability ("Playing Again", "Game Variation", "Non-Repetitive"), received a relatively low score compared to the other 3 sections which can be attributed to the low amount of minigames and its variations. On the other hand, the game's UI/Graphics ("Intuitiveness", "Navigation", "Graphics"), Responsiveness and Ease of Gameplay ("Difficulty", "Responsiveness", "Glitches/Bugs"), and Sense of Achievement ("Completion Pride", "High Score Pride") garnered positive ratings. This suggests that players found the game visually appealing, responsive, free from glitches/bugs, and rewarding in terms of accomplishment.

The survey also included a section where the playtesters had the opportunity to share additional comments and suggestions about the game. Common and notable feedback received from the players can be summarized as follows:

- Improve the clarity and simplicity of instructions to accommodate those with little to no tech experience.
- Minor tweaks in game mechanics such as the ability to select multiple suspicious sections in the Email Red Flags minigame.
- Increase the difficulty and challenge for the player by adding a timer.
- Maintain a consistent art direction for the game's UI and game elements since the game currently makes use of placeholder elements with both retro and minimalist styling.

- Shorten post-round messages so players don't need to read lengthy paragraphs.

Conclusions and Recommendations

Conclusions

The results of this study suggest that playing the game had a positive impact on the participants' interest in cybersecurity. However, it was not able to significantly affect their knowledge in cybersecurity. The game's UI/graphics, responsiveness and ease of gameplay, and sense of achievement was well received by the players while the game's replayability received the lowest rating among the various aspects of the gameplay experience. Certain adjustments to the game may be necessary to address the game's inadequacies and improve the game's overall quality and presentation.

Recommendations

Based on the average pre-test knowledge score of approximately 14.919, it is plausible that the lack of significant difference in cybersecurity knowledge is due to the magnitude of participants with prior knowledge and experience with cybersecurity concepts. Consequently, the game was unable to provide them with substantial new knowledge as they were already familiar with these concepts. In this regard, it would be beneficial to expand or create a more comprehensive test for the topics covered by the game. Additionally, to ensure a more representative sample of the general Filipino public, it is recommended to conduct playtesting with a larger number of participants, preferably those with little to no experience with cybersecurity and within a broader age bracket. By increasing the playtesting population, a wider range of perspectives can be captured. This expanded sample size allows for the utilization of various statistical tests. For instance, an Analysis of Variance (ANOVA) can be used to compare responses across multiple groups, such as individuals with different educational backgrounds or preferred languages.

In terms of the feedback obtained for the game, the researchers suggest providing the player with the option to change the game's prompts and instructions into their preferred language, in particular, English or Filipino. In addition, to address problems in replayability, it is recommended to create additional variations for the existing minigames and to develop minigames covering additional cybersecurity concepts.

The educational features of the game can also be expanded by implementing an in-game ”wiki” that allows for in-depth discussions on the topics tackled. This approach enables the post-minigame messages to be more concise, focusing on the essential details while omitting supplementary or unnecessary information. Should the player be interested in learning more about the topic, the wiki can serve as an optional but comprehensive resource for information.

After realizing the game's positive impact in enhancing cybersecurity literacy and interest among the Filipino public, it is strongly recommended for the game to be adopted by the Department of Information and Communications Technology (DICT). Deploying the game on a platform with extensive reach would allow for widespread accessibility and exposure to a diverse audience. This move would enable the game to maximize its potential impact in promoting cybersecurity awareness and education throughout the country.

Bibliography

[1] Lawrence Agcaoili. *Financial cyber attacks surge by 2,324% in 2020*. Jan. 2022. URL: https://www.philstar.com/business/2022/01/18/2154527/financial-cyber-attacks-surge-2324-2020.

[2] Anne Janyarae E. Arato et al. “Juan Piece, a Mobile Puzzle Game about Philippine Geography: its Effects on Students’ Problem Solving Skills”. In: *Proceedings of the 2019 International Conference on Mathematics, Science and Technology Teaching and Learning* (June 2019). DOI: 10.1145/3348400.3348401.

[3] Gene Marck B. Catedrilla et al. “An Android-based mobile educational game for disaster preparedness: An input to risk reduction management”. In: *Indonesian Journal of Electrical Engineering and Computer Science* 22.2 (May 2021), pp. 936–943. DOI: 10.11591/ijeecs.v22.i2.pp936-943.

[4] Sebastian Deterding et al. “From Game Design Elements to Gamefulness”. In: *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments* (Sept. 2011). DOI: 10.1145/2181037.2181040.

[5] Rhys Elliott. *The Philippines’ games market: Data and insights*. May 2020. URL: https://newzoo.com/insights/articles/data-and-insights-on-the-philippines-games-market.

[6] Maria Corazon G. Fernando et al. “Trash Attack: A 2D Action Puzzle Video Game to Promote Environmental Awareness and Waste Segregation Behavior”. In: *International journal of simulation: systems, science & technology* 20.2 (2019), pp. 1–4. DOI: 10.5013/ijssst.a.20.s2.24.

[7] Maurice Hendrix, Ali Al-Sherbaz, and Victoria Bloom. “Game based cyber security training: Are serious games suitable for cyber security training?” In: *International Journal of Serious Games* 3.1 (Mar. 2016). DOI: 10.17083/ijsg.v3i1.107.

[8] Ute Ritterfeld, Michael J. Cody, and Peter Vorderer. “Introduction”. In: *Serious games: Mechanisms and effects*. Routledge, 2009, p. 6.

[9] Anthony M. Rivadulla et al. “PhilLoveHistory: Enhancing knowledge in Philippine history using Mobile Game Application”. In: *TENCON 2017 - 2017 IEEE Region 10 Conference* (Nov. 2017), pp. 817–821. DOI: 10.1109/tencon.2017.8227971.

[10] Microsoft Philippines Communications Team. *Cybersecurity threats to cost organizations in the Philippines US $3.5 billion in economic losses*. May 2019. URL: https://news.microsoft.com/en-ph/2018/06/01/cybersecurity-threats-to-cost-organizations-in-the-philippines-us3-5-billion-in-economic-losses/.