International Journal of Data Science and Advanced Analytics (ISSN: 2563-4429)

Evaluating the Effectiveness of Gamification to Increase Cybersecurity Awareness among Students

Amos Alban Jr Maluda[1], Intan Farahama Binti Kamsin[2], Zety Marlia Zainal Abidin[3], Hemalata Vasudavan[4]

Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia.

[1]tp062043@mail.apu.edu.my, [2]intan.farahana@staffemail.apu.edu.my, [3]zety@staffemail.apu.edu.my, [4]hemalata@staffemail.apu.edu.my

***Abstract*— Cybersecurity is a field that is in constant motion due to the nature of cyberthreats which are always finding ways to abuse vulnerable victims. The victims are not discriminated which means that even youths are being targeted – to take advantage of their lack of awareness in cybersecurity. To counter this, there are some efforts to increase awareness through gamification. This is because games are fun, interactive, and appealing to the youths, which can help motivate them to put in effort to learn. Therefore, this paper aims to create a solution that can evaluate the effectiveness of this gamification process. There will be target users that will be sampled with the proper method to choose the right respondents to get data from them through a data collection method. In the end, with this paper – the potential of gamification to meet educational objectives can be uncovered.**

***Index Terms* – Awareness, Cybersecurity, Gamification, Students.**

1. Introduction

This proposal paper serves to go over an issue that is present in the cybersecurity field. Cybersecurity refers to the protection of computer related systems and sensitive information from unauthorized disclosure, modification, or deletion [1] However, not many are aware of this, including the practices to lower the chances of becoming victim to cyberattacks. Especially among the youths. There has been various effort done to expose cybersecurity and its practices, in both traditional and modern teaching style. Traditional inthis case is referring to the introduction of cybersecurity related modules in education. This is done for the students to experience and be exposed to cybersecurity through theoretical, classroom based, teaching methods. This is a tried-and-true method that we can already expect the effectiveness of. On the other hand, there are also some efforts ofraising awareness through the process of gamification. Essentially, this means that students are taught through games that can simulate real world challenges, prompting them to solve issues ina more practical and hands-on manner. Additionally, it is also a form of entertainment that can be appealing to the youths and motivate them to put more individual effort in playing while learning at the same time. Nonetheless, it is still a new strategy that has not been implemented on a larger scale. Therefore, this proposal paper will go over the method of effectively evaluate this gamification strategy to provide insight and understanding to the potential value of increasing awareness through games. Doing this would benefit both cybersecurity and education sector by producing cybersafe students and realise the impact of gamification for studies.

This document will go over the literature review of the considered domain that are found by researching through related journal articles. Then, similar systems is discussed where inspiration of potential features are gathered to be implemented in the proposed solution. The document continues by discussing about the problem that needs to be addressed as well as the aim, objectives, and significance of this research to solve the problem stated. Also included is the methodology for this study to serve as a guideline to collect the correct data from the right respondents. In the end, there will be an overview of the proposed system that is the solution for the problems, and the main aspect of this proposal paper.

2. Literature Review

2.1 Research Domain

2.1.1 Cybersecurity Awareness among Youths

It is not of a surprise that youths are becoming more familiarized with the internet and their devices. However, this familiarity does not equal to their awareness level of cybersecurity. In a research study done by [2] – they reported that respondents around the age of 8- 12 years could only answer about 19% of the survey questions that evaluates their cybersecurity awareness. Additionally, they also mention that common cybersecurity terms as well as awareness of

common threats like phishing, were unfamiliar to students of the survey. A study by [3] from 2016, stated that ignorance in handling private and public information are causing cyber threats to increase, which endangers more than just the students. Moreover, it is even riskier when improving awareness among students concerning issues and practices in cybersecurity is not being actively approached by educational institutes [4]. Some studies have also concluded that the amount of time students spend interacting with the internet or their devices does not contribute to increasing cybersecurity awareness [5][6].

Therefore, the information gathered from the articles relating to the cybersecurity awareness among youths shows that there is an alarmingly low awareness level of aspects related to cybersecurity. The aspects is in regards to common practices and threats. This then contributes to the increase of cybercrime threats, due to the vulnerability of those youths. That is why this research study will be done to help increase the cybersecurity awareness to reduce cyberthreats.

2.1.2 Increasing Cybersecurity Awareness through Gamification

To increase cybersecurity awareness, some have opted into educating through gamification. In 2019, [7] created a mobile game with a role-playing quiz genre that is designed to teach users about password security. They highlighted that users find the game to be enjoyable and in turn, were able to benefit from it. Whereas [8], stated that gamification is a betteralternative that solves certain weaknesses in existing trainings to increase cybersecurity awareness, especially when it comes to motivation and engagement. In his research, he was able to gamify the trainings and obtained satisfactory results. Additionally, [9], mentions that information system educators can opt for gamification – because they are entertaining, fun, and appealing to students. They elaborated that games are also an alternative to deliver learning objectives of an area of study. In 2021, [10]created a cybersecurity game that consist of four levels which vary in cybersecurity practices – concerning password, phishing, social engineering, and physical security. They also added that the gamewas reported by the users to be better than traditional methods to increase awareness. Other than that, using the Octalysis gamification framework, a virtual cybersecurity escape room was created – which resulted in improvement of knowledge retention as well as user involvement [11].

Therefore, from the studies done by the researchers above, it can be understood that gamification of cybersecurity awareness can bring high potential in being appealing and more effective to create a more cybersafe community. However, the target users of the gamification were mostly employees that are matured and experienced. That is why this research study will evaluate the gamification done on students to get better insight on the effectiveness of doing so.

2.2 Similar System

2.2.1 picoCTF

The first system is called picoCTF. This is a website that is designed to be a computer security exercise. Users are required to solve challenges in a capture the flag format in various types of challenges. These challenges are ranging from web and binary exploitation, reverse engineering, cryptography, forensics, and general skills. Users will need to use their cybersecurity knowledge to take advantage of vulnerabilities of the system within the challenges to get the flag. Additionally, picoCTF offers a safe and legal method to learn about cybersecurity as the challenges are designed to be hackable [12].

Figure 1: Progress Overview in picoCTF

Figure 1 above shows what a teacher can see regarding the information from their students. This system allows teachers to monitor the activity of the students by being able to know the number and type of challenges that they have done. Not only that but being able to solve challenges can help determine that knowledge level of the users regarding cybersecurity and common exploitation techniques.

2.2.2 usecure

This is an application called usecure, developed by a company with the same name. This company refers to themselves as a world-leading solution to Human Risk Management. The solution is done through the usecure app which is designed to monitor, measure, and mitigate cyber risk of employees [13]. This application can estimate the risk percentage of each individual to provide them with resources and trainings that can increase their cyber awareness to reduce the risk. In addition to that, this app also offers a simulation of phishing attacks to ensure employees are always aware of common attacks. Moreover, usecure is also able run exposure checks in the dark web to identify whether the employee credentials have been compromised.

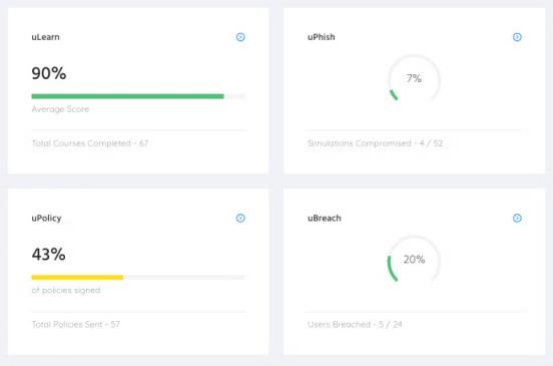

Figure 2: Progress Overview

Figure 3: Risk Analysation

Figure 2 shows the progress rate of an employee based on their completion of the activities in the application. The data gathered from this is analysed and used to create an estimation of risk percentage. This feature to analyse data is important to ensure less manual labour done to gather insight and information about the risk level of the company from being attacked, due to the lack of cyber awareness in employees.

2.2.3 Comparison Table

Features	picoCTF	usecure
Monitor activity function	✓	✓
Retaining knowledge function	✗	✓
Cybersecurity knowledge testing	✓	✓
Analysation of data function	✗	✓
Free	✓	✗

Table 1: Comparison Table between Similar Systems

Table 1 shows the comparison of the features between the similar systems that are mentioned above. The considered features for this comparison table includes the function to be able to monitor the activity of the users. This is important to check the progress of the users to see if they are putting sufficient effort. Next, is the function to retain knowledge that they learn. Being able to do this function helps to ensure that users are always aware of the potential threats in whatever they do. Whereas the cybersecurity knowledge function is to test whether the users have enough knowledge about cybersecurity, which includes the good practices and common attack techniques. Not only that but the function to analyse data is also important to reduce manual labour and help in understanding and getting insight from the data. Lastly, a feature to consider is the price. It is good if the price is low, better if it is free – to provide everyone with the availability to this resource. The usecure application has the most check marks at 4, while picoCTF only has 3. However, it is extremely important to note that compared to usecure, picoCTF is a free system. Therefore, the system that is proposed in this paper will be created to fill in the gaps within the two similar systems to create a better solution that has all the considered features.

3. Problem Statement

Currently, where technology is becoming part and parcel of life, we can see that the youth are becoming increasingly exposed to the internet; to the point of becoming potential targets for attackers [14]. Reference [14] further elaborated on this by stating that many youths fall victim to malicious activities which leads to varying consequences. Whereas, in 2020 – [15], specifically mentions that Malaysian are no strangers to internet addiction due to the effectiveness and implementation of information and communication technology (ICT).

To increase cybersecurity awareness among youths, many researchers propose the implementation of games; in hopes of appealing to them. Gamification of educational objectives are becoming a new strategy to teach in an individual level, while incorporating fun and entertainment -to further enhance the effectiveness of teaching [16]. However, not much research has been conducted to fully evaluate the effectiveness of increasing cybersecurity awareness through this gamification process. Thus, this research proposal acts to propose a method to find out whether the gamification of cybersecurity awareness is worth pursuing.

4. Research Aim

The aim of this research is to propose a solution in the form of an application that can provide thorough analyzation and evaluation of the effectiveness of using games to increase and retain cybersecurity awareness among students by focusing on the following objectives.

5. Research Objectives

- To create an application that can monitor student activity.
- To create a method to ensure retention of the cybersecurity awareness.
- To test the performance of students relating to cybersecurity after the gamification process.

6. Research Significance

This research is significant to ensure that the youths of the world today can protect themselves from cyberthreats. Having the knowledge of common techniques used by cybercriminals will be beneficial to ensure that the youths, and anyone around them – do not become victims. Not only that, but ensuring the population becomes aware of cybersafe practices will greatly aid those in the cybersecurity field in repelling any potential threat attacks, that are targeting vulnerable youths. Moreover, this study is also significant to encourage the ministry of education to take initiative in gamification to meet educational objectives. Thus, in the long run – potentially creating a safer world with highly cybersafe individuals.

7. Methodology

There will be two target user types involve in sampling which are educators and experts. The educators are those in the cybersecurity field. It necessary to get the inputs of the educators in this field to properly evaluate the students in the correct aspects. This way, the proposed application can provide the right insight and information whether the student is learning well. Whereas the experts will be those who are professionals in designing applications. The purpose of having these experts as target users is to determine best design and implementations to help achieve the objectives efficiently and effectively.

The sample size for each target users will be 10 samples to ensure that sufficient information can be gathered to fulfill the objectives. The sample will come anyone in Malaysia, in any state, to ensure that plenty knowledge can be gathered from respondents with different backgrounds.

There will be two sampling methods used to choose the respondents from both target users. The methods are both qualitative and non-probability styled. The first target users - the educators, will be sampled using quota sampling. Only those who have 3 or more years of experience as an educator in cybersecurity will be sampled. This allows the process of retrieving data to be fast and easy, while also being cheaper due to specifically filtering the users [17]. The second target users – the application design experts, will be sampled through the self-selection method. This is done by publicly announcing the need for those professionals to be involved in research, using social media applications.

The data collection method that will be used is in the form of a semi-structured interview. This method requires predetermined and spontaneous questions to be asked during the interview. Additionally, a semi-structured interview is the best for this situation to be able to understand in depth and fully gather sufficient data to be used for analysis.

8. Overview of the Proposed System

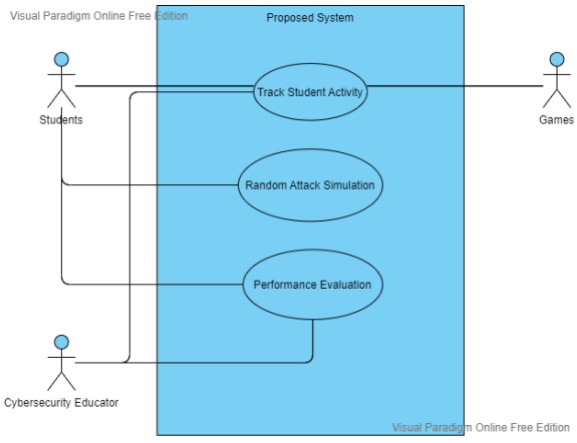

Figure 4: Proposed System Use Case Diagram

Figure 4 above shows the use case diagram for the proposed system that this proposal paper aims to create. In summary, there are three actors involved in the proposed system. The actors are students, cybersecurity educators, and games. Students in this case are those who are increasing their cyber awareness through games. Whereas the games actor are all the gamification games that helps to increase cybersecurity awareness. The games will be integrated into the proposed system so that the student activities can be tracked and monitored. Lastly, the cybersecurity educators are the actors who will be assessing the result of the gamification process. They will have access to the performance evaluation of the students. This can give them information and insight whether the gamification process is effective in increasing cybersecurity awareness. Additionally, the proposed system also includes random attack simulations. This is to ensure that the students are always aware of attacks that can happen anytime. However, it should be noted that this is the barebone structure of the proposed system. After getting data from the application design experts, certain design aspects as well as any modification to the use case diagram is expected.

9. Conclusion

This proposal paper serves to go over the need to evaluate the gamification process to help in increasing cybersecurity awareness among students. An application is proposed to give insight and information regarding the performance of the students after going through the gamification process. The data gathered from this will show the effectiveness of using games to increase cybersecurity. Thus being able to realise the potential of using games for education reasons.

References

[1] Shea, S., Gillis, A. S., & Clark, C. (August, 2021). *What is cybersecurity?* Retrieved from TechTarget : https://www.techtarget.com/searchsecurity/definition/cyberse curity#:~:text=Cybersecurity%20is%20the%20protecti on%2 0of,centers%20and%20other%20computerized%20sys tems

[2] Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016, December). A survey on Internet usage and cybersecurity awareness in students. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)* (pp. 223-228). IEEE.

[3] Peker, Y. K., Ray, L., Da Silva, S., Gibson, N., & Lamberson, C. (2016, October). Raising cybersecurity awareness among college students. In *Journal of The Colloquium for Information Systems Security Education* (Vol. 4, No. 1, pp. 17-17).

[4] Moallem, A. (2018, July). Cyber Security Awareness Among College Students. In *International Conference on Applied Human Factors and Ergonomics* (pp. 79-87). Springer, Cham.

[5] Potgieter, P. (2019). The Awareness Behaviour of Students On Cyber Security Awareness by Using Social Media Platforms:

[6] Subramaniam, S. R. (2017). Cyber security awareness among Malaysian pre-university students. E. *Proceeding of the 6th Global Summit on Education*, 1-14.

[7] Scholefield, S., & Shepherd, L. A. (2019, July). Gamification techniques for raising cyber security awareness. In *International Conference on Human-Computer Interaction* (pp. 191-203). Springer, Cham.

[8] Rieff, I. (2018). Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach.

[9] Nwokeji, J. C., Matovu, R., & Rawal, B. (2020). The use of Gamification to Teach Cybersecurity Awareness in information systems.

[10] Abu-Amara, F., Almansoori, R., Alharbi, S., Alharbi, M., & Alshehhi, A. (2021). A novel SETA-based gamification framework to raise cybersecurity awareness. *International Journal of Information Technology*, *13*(6), 2371-2380.

[11] DeCusatis, C., Gormanly, B., Alvarico, E., Dirahoui, O., McDonough, J., Sprague, B., ... & Mah, B. (2022, January). A Cybersecurity Awareness Escape Room using Gamification Design Principles. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0765-0770). IEEE.

[12] Owens, K., Fulton, A., Jones, L., & Carlisle, M. (2019). pico- boo!: How to avoid scaring students away in a ctf competition.

[13] usecure. (2022). *The world's leading Human Risk Management (HRM) solution*. Retrieved from usecure: https://www.usecure.io/en/about

[14] Smith, D. T., & Ali, A. I. (2019). YOU'VE BEEN HACKED: A TECHNIQUE FOR RAISING CYBER SECURITY AWARENESS. *Issues in Information Systems*, *20*(1).

[15] Zulkifli, Z., Abdul Molok, N. N., Abd Rahim, N. H., & Talib, S. (2020). Cyber Security Awareness Among Secondary School Students in Malaysia. *Journal of Information Systems and Digital Technologies*, *2*(2), 28–41. Retrieved from https://journals.iium.edu.my/kict/index.php/jisdt/article/view/ 151

[16] Qusa, H., & Tarazi, J. (2021, January). Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students. In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0677-0682). IEEE.

[17] Glen, S. (22 August, 2021). *Quota Sampling: Definition and Examples*. Retrieved from Statistics How To: https://www.statisticshowto.com/quota-sampling/