Towards Enhancing Cyber Security Awareness Using Gamification Escape Room

1st Basil Alothman,2nd Khaznah Al-Khulifa, 3rdReem Al-Shammari, 4th Chibli Joumaa, and 5th Murad Khan
Department of Computer Science and Engineering
Kuwait College of Science and Technology(KCST)
Kuwait-City, Doha District
1st,b.Alothman@kcst.edu.kw, 2nd 171001@student.kcst.edu.kw, 3rd r.alshammari@kcst.edu.kw,
4th c.Joumaa@kcst.edu.kw, 5th m.Khan@kcst.edu.kw

***Abstract*—The cyber-attacks are becoming more complex and prevalent, therefore, there is a need for raising cyber security awareness to educate and defend people about the latest hacking attacks by using creative and efficient education methods. Similarly, gamification escape rooms have acquired popularity as a cutting-edge and efficient way to increase cybersecurity awareness and individuals' abilities to identify, avoid, and respond to cyber risks. The proposed approach includes developing a cybersecurity escape room on a website or application that uses gamification and puzzle-solving tasks to mimic actual cyber-attack scenarios. The cybersecurity escape room offers a virtual setting where users can practice cybersecurity techniques and learn to prevent potential security attacks from attackers, creating a secure and educational environment where users can gain experience and learn the skills, they need to deal with real-life hacking situations. By using this method, users can have fun and experience the adventure of a cyber threat scenario while making informed decisions and raising their security awareness.**

***Index Terms*—Cybersecurity awareness, cyber escape room, gamification, educational**

I. Introduction

To educate and raise cyber security awareness for employees and new joiners for a company, it will be difficult to educate them and understand the threat of different cyber-attacks like phishing, spear-phishing, and scams. Cyber education scientists started to educate general employees and people to raise their awareness through innovation in education. In this regard, the cyber escape room is an idea to promote security-related concepts with the employees and students. In addition, using the cyber security gaming escape room helps employees, internet and computer users, or anyone who works on a computer or smartphone using the internet. Further, it protects those who are vulnerable to security issues and different types of attacks that lead to preventing them from unknown hacking by raising awareness through questions and real-life examples. The cyber security gaming room is an educational course simplified in a fun, smooth and easy way. With the spread of cyber security gaming rooms, we can introduce users to computer devices, whether they are students, employees, or anyone who works on the computer using the Internet about security problems and attacks. Similarly, it can guide them on how to avoid security threats and necessary steps to maintain the safety of the user device and how to avoid exposure to damage. With the development of technology and the increase in its uses in all fields we are living in a world that is continually evolving and where modern conflicts have moved to the cyber domain [1], the situation of devastating attacks on computers increased. Most users of computers and the internet do not understand the danger of these attacks. Similarly, due to the lack of knowledge and ability to quickly respond to attacks, it is necessary to provide users with security practices [2]. In order design an educational cyber escape room, there a number of challenges are associated with it. For instance, people of different ages will be divided into groups based on their level of expertise, security questions preparations, etc. In this paper, we provide proof of a concept of a cyber escape room to guide and educate people of different ages related to common security issues such as phishing, physical security attacks, hijacking, etc. The proposed cyberscape room provides a gaming environment for a user to interact with the participants and the players in it. The user can learn the basics of cybersecurity. Similarly, in advanced stages, the user learns the complex matters of cybersecurity such as the understanding of the methods of acquiring information and benefiting from it and promoting the thinking and understanding process, etc. The proposed game covers the basics, including knowing the importance of having an antivirus, firewall, and complex password work. Similarly, the user can know how to avoid all of the spyware, adware, and phishing attacks. The paper is divided into different sections. Section II explains the related work followed by the proposed system working mechanism in Section III. Finally, the conclusion is given in Section VI.

II. Related Works

This segment discusses briefly the efficiency of gamification escape rooms in raising cybersecurity awareness. Numerous recent studies show that gamification improves cybersecurity training by increasing participation, motivation, and retention of knowledge. The research studies in [3], propose Cyber-Hero which is a gamification system targeted at raising high school students' cyber security awareness. The framework incorporates cyber security challenges, points, and badges into a learning management system, allowing students to

compete in cyber security assignments. Moreover, the article [4], presents a Cyber Security Awareness Game (CSAG) for secondary school students. To boost students' awareness of cybersecurity, the game includes a story-based approach with multiple security-related situations and quizzes. The design of the game emphasizes usability, engagement, and gamification aspects such as rewards and feedback. More real-world situations may be valuable in demonstrating the necessity of cybersecurity in everyday life. To increase the efficacy of the Cyber Security Awareness Game.

Moreover, in the article [5], the authors created a set of games to teach players about various advanced persistent threat (APT) situations, which are becoming more common in cyber systems.While the study claims that the suite of learning games increased players' capacity to recognize and respond to advanced persistent threats (APTs) when compared to traditional training techniques, the training impact may vary depending on the game design quality.Improving the accuracy and variety of simulated cyber-attack scenarios, as well as enhancing machine learning trained and optimized models for cybersecurity by using high-quality datasets should be taken into consideration to guarantee the effectiveness of this approach.

The research study in [6] suggests a novel approach for increasing cyber security awareness by developing a complete cyber security awareness program introducing an interactive video game, Cyber Shield Game that includes a variety of training materials and methods, such as classroom instruction, online learning modules, and simulation drills. Password security, malware protection, and online privacy, among other topics, are covered scenarios in this interactive and engaging designed game. To improve its efficacy in raising users' cybercrime knowledge, research could include adding levels on social engineering and phishing to the Cyber Shield game, as well as incorporating a chatbot for improved feedback during gaming. Similarly, there are several techniques to gamified cybersecurity training presented in [7]. However, those schemes are still requiring high-end computation and programming to implement.

In addition, CyberCIEGE is a virtual cybersecurity training platform that is used to teach students and workers in cybersecurity by academic institutions, government agencies, and private organizations [8]. It involves identifying vulnerabilities and failures, devising a defense and security plan, identifying risky behaviors, and analyzing a set of samples to identify possible phishing emails. The game can be improved by adding more recent and advanced cyber threats and attacks, as well as improving the game's usability and user-friendliness, to make it simpler for players to learn and navigate the game.

These studies suggest that by integrating virtual reality and escape room activities to simulate real-world settings, gamification may provide practical, hands-on experience in detecting and responding to cybersecurity dangers. Paper [9], presents a digital game called PenQuest Reloaded which is based on MITRE ATTACK, D3FEND, and the NIST SP 800-53 security standard to develop cyber security capabilities in technical education especially cyber defense skills in protecting a computer system.To minimize any possible lack of effectiveness, it is critical to assess the framework's potential limits and to regularly review its impact and effectiveness on students' learning and conduct.

The research findings in the article [10] utilized a similar approach using gamification elements such as points, badges, levels, and leaderboards to engage and motivate players. The game combines many cybersecurity issues, such as password security, phishing attacks, and malware prevention. Both papers can increase engagement, retention, and motivation yet potential downsides include restricted scope, game addiction, and implementation issues such as the requirement for skilled instructors and expensive development and maintenance costs may occur.

Recent studies have investigated the potential of gamification in enhancing cybersecurity risk management, cyber hygiene, and threat intelligence, in order to improve users' cybersecurity knowledge, skills, and habits [11], [12], and [13].

Based on the research examined, gamification escape rooms offer the potential as a unique and efficient method of increasing cybersecurity knowledge and preparation. However, further study is required to evaluate the long-term effectiveness of gamification escape rooms as well as to evaluate their possible applications in other industries and settings.

III. Proposed Methodology

In this paper, we proposed a cyber security game in the form of an escape room through which a user is provided with a simulation of a real-time security attack scenario. The user learns from the simulation how to use the knowledge and improve it while interacting with a game. Further, the user gains an experience of how to apply the knowledge obtained in the proposed escape room in the field of work. For instance, how to deal with situations when your colleagues or friends ask you to give them your computer username and password. Similarly, the proposed system offers an environment for dealing with the latest security attacks such as phishing, hijacking, etc. The proposed escape room is built in a way to educate a user to obtain enough information while playing the game to successfully avoid such security attacks in the future. Security awareness through the proposed game allows people to have a fun time while learning and feel a sense of engagement. Similarly, the proposed scheme shows results of the brain of a user being more actively involved when playing the proposed game. Through the proposed simulations and games, people of every age can learn to appreciate failure as a learning opportunity. Similarly, the reward at the end of a successful attempt provides a more engaging environment. In addition, we provide an operating environment that secures the attached devices from any sort of security attack while the user is busy playing a game. Because the cyber-attacks are mostly due to human errors and lack of knowledge. In the proposed escape room, a player is the main and ultimate user

of the game. Initially, the player of the game is provided with a VR device.

In the proposed system, we define the problem clearly to present a cyber security methodology through the escape room. Basic education is provided to the user in the beginning with the basics of cybersecurity. We believe that complex concepts cannot be learned without understanding the simplest first. Therefore, the proposed game initially interacts with the players to learn the basics of cybersecurity. Similarly, in the last stages, a user is provided with more complex scenarios to meet and understand the methods of acquiring information and benefiting from it. This includes thinking, understanding, and then reminding. The game covers various topics of cyber security such as antivirus, firewalls, and complex passwords. It also provides knowledge related to spyware, adware, and phishing attacks. The flowchart diagram in Figure 2 displays the process when the player enters a gaming place. As the player arrives at the game place, a support staff member guides the player regarding the roles of playing the game. Similarly, the player starts the game after the staff member closes the door of the escape room. The game interacts with the player and if the player's response is correct, the player is awarded winning points. However, if the player responded with a wrong answer, the player loses the game and leaves the room.

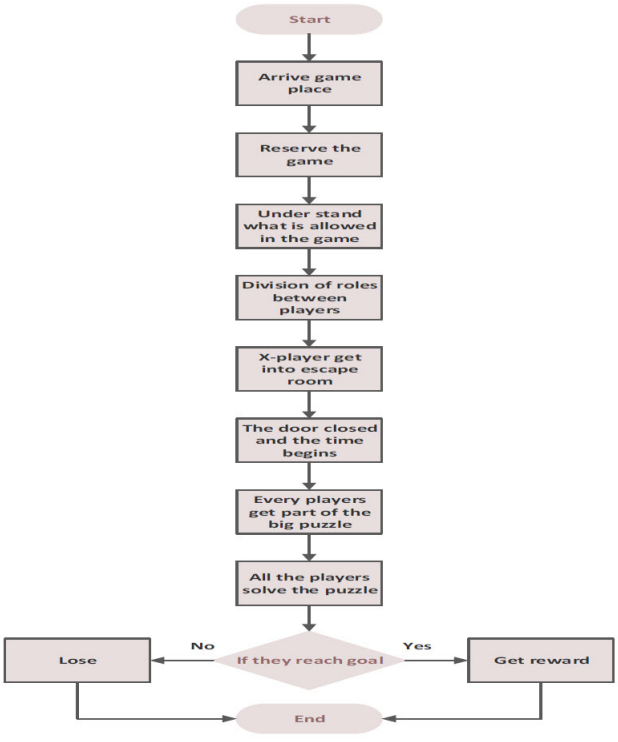

Fig. 1. Cyber Security Escape Room Flowchart

IV. Conclusion

In conclusion, we have many cyber security tools that will help to enhance cyber security activities within organisations like cyber security awareness, training, education, policy, governance, and cyber security technology. In this paper, we focused to enhance cyber security awareness using a gamification escape room to enhance cyber security awareness user experience level to change user's cyber security defense behavior and apply it in their work to protect IT infrastructure from end-user attacks. In future work, we would like to invest to enhance the graphical interface with a more local cartoon character to act the attacks and keep them more friendly to use and discover more IT security attack techniques to add more questions and answers with attacks critical thinking.

References

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] H. Qusa and J. Tarazi, "Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students," 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), NV, USA, 2021, pp. 0677-0682, doi: 10.1109/CCWC51732.2021.9375847.

[4] L. W. Shen, H. K. Mammi and M. M. Din, "Cyber Security Awareness Game (CSAG) for Secondary School Students," 2021 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, 2021, pp. 48-53, doi: 10.1109/ICoDSA53588.2021.9617548.

[5] T. Zhu, D. Ye, Z. Cheng, W. Zhou and P. S. Yu, "Learning Games for Defending Advanced Persistent Threats in Cyber Systems," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, doi: 10.1109/TSMC.2022.3211866.

[6] F. Abu-Amara and H. Tamimi, "Cyber Shield Security Awareness Program," 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2021, pp. 422-425.

[7] S. Alma'ariz, R. B. Hadiprakoso, Girinoto and N. Qomariasih, "Soceng Warriors: Game-Based Learning to Increase Security Awareness Against Social Engineering Attacks," 2022 IEEE 8th Information Technology International Seminar (ITIS), Surabaya, Indonesia, 2022, pp. 124-129, doi: 10.1109/ITIS57155.2022.10009041.

[8] "Cyber CIEGE." https://nps.edu/web/c3o/downloads (Accessed February 25, 2023.)

[9] A. Chattopadhyay, C. Maschinot and L. Nestor, "Mirror Mirror On The Wall - What Are Cybersecurity Educational Games Offering Overall: A Research Study and Gap Analysis," 2021 IEEE Frontiers in Education Conference (FIE), Lincoln, NE, USA, 2021, pp. 1-8, doi: 10.1109/FIE49875.2021.9637224.

[10] R. Luh et al., "PenQuest Reloaded: A Digital Cyber Defense Game for Technical Education," 2022 IEEE Global Engineering Education Conference (EDUCON), Tunis, Tunisia, 2022, pp. 906-914, doi: 10.1109/EDUCON52537.2022.9766700.

[11] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[12] Wu T, Tien KY, Hsu WC, Wen FH. Assessing the Effects of Gamification on Enhancing Information Security Awareness Knowledge. Applied Sciences. 2021;11(19):9266. doi:https://doi.org/10.3390/app11199266

[13] Naeini, F. F., Maleki, H., and Badamchi, M. R. (2019). A Gamified Escape Room for Cybersecurity Awareness Training. In 2019 3rd Conference on Technology of Internet of Things (TechIoT) (pp. 76-80). IEEE.