2024 Third International Conference on Distributed Computing and High Performance Computing (DCHPC) | 979-8-3503-8158-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/DCHPC60845.2024.10454080

Promoting Cybersecurity Knowledge via Gamification: An Innovative Intervention Design

Fatokun Faith B.
Malaysian Institute of Information Technology,
Universiti Kuala Lumpur
Kuala Lumpur, Malaysia
evangfatoks@gmail.com

Zalizah Awang Long
Malaysian Institute of Information Technology,
Universiti Kuala Lumpur
Kuala Lumpur, Malaysia
zalizah@unikl.edu.my

Suraya Hamid
Department of Information Systems, Faculty of Computer Science & IT,
Universiti Malaya
Kuala Lumpur, Malaysia
suraya_hamid@um.edu.my

***Abstract*— Cybersecurity is becoming a critical challenge as technology thrives with novel innovations. The increase in cyber threats is quite alarming. Cyber-users' vulnerability is a serious issue as negligent behaviour alongside a lack of basic cybersecurity knowledge constitutes a major cause of attacks today. Several approaches have been introduced via security systems to provide prevailing defence against numerous cybersecurity attacks. However, they are relinquished to limited impact due to a lack of compliance with security guidelines by end-users deficient in basic cybersecurity knowledge. Gamification has played an important role in educational contexts as it promotes motivation and engaging learning. Though still a new research field, literature has postulated that the innovative application of gamification in cybersecurity could be a winning strategy to combat cybersecurity threats. This paper, via an experimental/qualitative approach, proposes a comprehensive cybersecurity gamification design based on established gamification theories to ensure the validity of the cybersecurity gamification tool. The cybersecurity gamification tool is aimed at promoting the cybersecurity knowledge of end-users. Gamification design has the potential to transform a training environment by altering the player's emotional experience alongside their social position and sense of identity. Gamification, if implemented properly, can impact beyond just learning but also boost knowledge, learning experience and engagement of the targeted audience through motivation by the game elements. This research is ongoing and the result of a survey evaluating the impact of the gamification tool in promoting cybersecurity knowledge will be presented in a future publication.**

Keywords*— *Cybersecurity, Gamification, Cybersecurity Knowledge, Online Safety, Cybersecurity Gamification

I. INTRODUCTION

Cybersecurity is recently becoming a field of high interest among researchers as well as a major issue in society. Recent cyber-attacks on high profiles have set a pace for society to comprehend the urgent need to preserve the security of both computer systems and the Internet, in concordance with preventing malicious attacks on various sectors, with the inclusion of securing the weakest link in cybersecurity, which are humans [1]. Cyber-users have gradually been seen as the major reason for most vulnerabilities that occur in security which could compromise an entire network via negligent or erroneous behaviours. Also, the lack of basic cybersecurity knowledge is also responsible for the high rate of cybercrime victimization across the globe today. User vulnerability is a critical challenge due to the limitations in knowledge by individuals regarding cybersecurity guidelines and warnings. Despite the provision of powerful defence by existing security systems against a lot of cybersecurity attacks, the effect is still minimal if there is no proper compliance with the security guidelines by users [2, 3]. Therefore, there is a need to invest in innovative education and immersion of cybersecurity knowledge among the general populace to ensure their safety. Students, in particular, are a special target group for cybersecurity knowledge promotion as they are at a stage where experimental learning could help retain long-term knowledge [4, 5]. From the angle of education, gamification, both as a tool for experimental learning as well as absorbing research learning experiences, can aid the improvement of other essential skills. Such skills comprise setting goals, cooperation, and self-efficacy. Moreover, gamified systems have the potential to adapt a couple of practical skills alongside multiple learning theories, such as decision-making activities and problem-solving [6], despite the possible concerns regarding their usage, respectively. Among the major concerns is the inadequacy of knowledge linked to the level of feature effectiveness in game design to improve the performance of the game.

Daily, cyber-attacks and cybercrime are increasing at a rapid frequency. Moreover, cybersecurity is a major challenge for both the public and private sectors. There is a high demand for more experienced security experts in the workforce [6]. Nevertheless, it is important that these workers are well-equipped with adequate knowledge that can help them tackle basic cybersecurity issues. Massive attention is driven towards the behavioural aspect of cybersecurity of recent. This often leads to severely crucial cyberattack repercussions. Data breaches or hacking have the potential to cause major economic or reputational damages, thus resulting in a lack of trust in the affected firms [6, 7]. Contemporarily, companies of different sizes are constantly being attacked and probed because of numerous high-profile cyberattacks. It is, therefore, essential to propose innovative ways of promoting cybersecurity knowledge, one of which is gamification to help curb the menace caused by vulnerable cybersecurity systems. The initiative behind using games to enhance teaching is not new. However, it remains one of the most efficient approaches to learning and educating [8-10]. Therefore, gamification is an excellent learning method. There are several definitions of gamification, but among all, most authors agree that gamification is "the application of gamely elements or mechanics to contexts or scenarios that are non-

979-8-3503-8158-0/24/$31.00 ©2024 IEEE

gamely with the sole purpose of inducing engagement alongside raising motivation levels [2, 8, 11], of which the application of such aspects is tantamount to engaging a user in learning.

Consequently, there is no cybersecurity assurance for the data of cyber-users, thereby leading to widespread cyberattacks, which makes national security vulnerable to probable threats [6, 12]. A couple of approaches are explored by diverse research in the cybersecurity domain, however, many of these approaches focus on traditional methods of training, providing little or no effect to reduce cybersecurity victimization. Some of the well-versed approaches to curb cyberattacks as represented in cybersecurity literature include challenge-based learning – where participants receive series of challenges on specific domains/field [13], awareness campaigns [14], table-top games [14, 15], among others. Moreover, another trending approach is serious games implementation. Unlike regular games, a serious game is aimed primarily at learning facilitation among participants/users rather than enjoyment/entertainment [15, 16]. However, there is a need to blend serious games and gamification into cybersecurity to ensure an immersive learning process which is inclusive of both entertainment and knowledge acquisition. Gamification of cybersecurity can perfectly replace regular safety trainings, thereby giving users the opportunity to consider various scenarios prior to facing them as normal daily activities [2]. According to literature, it has been asserted that cybersecurity is a topic that provides a suitable platform for training to be provided via serious gaming such as learning concentrated gamification [3, 8, 11]. Although, most studies considering this field of research are usually limited to small sample sizes as well as finding it difficult to strike a balance between how serious a cybersecurity game should be and for the choice of targeted audience. Thus, there remains a large gap regarding how gamification can be applied in the field of cybersecurity.

Regarding cybersecurity knowledge, literature stress more on the need for practitioners and analysist in the field of cybersecurity to possess expanse knowledge of cybersecurity and network operation [17, 18]. However, such knowledge is more specific oriented as the experts need such knowledge to detect and combat cyber-attacks. The end-users, nevertheless, who will eventually use internet and computers need to be equipped with basic and general cybersecurity knowledge to stay on the defensive side of cybersecurity. Unfortunately, innovative approaches that can help promote cybersecurity knowledge are lacking while the demand is higher today due to the high rate of cyberattacks. However, there is no clarity as to if acquiring detailed and deep cybersecurity knowledge constitutes the major determining factor of performance in dealing with cyberattacks. Research [18] show that individuals who possess diverse knowledge levels in cybersecurity alongside years of experience, might probably have different cybersecurity mental models. The higher the proficiency in cybersecurity, the possibility of a more efficient performance in detecting cyber-attacks as compared to lower knowledge levels. Thus, cyber-users who possess adequate cybersecurity knowledge are expected to make informed decisions when faced with cyberthreats as compared to those with limited knowledge. Gamification therefore is a perfect approach that can be used to promote cybersecurity knowledge to different level of expertise, as it can provide immersive learning and understanding of cybersecurity concepts while incorporating fun elements to make the learning process engaging.

Computer games are unique such that they offer an inclusive environment comprising features of aesthetic beauty, immersivity, and interactivity, thereby ensuring that complicated problematic aspects are explored in both an amusing and serious way. Moreover, research reveals that the majority of users find games to be entertaining as well as an effective technique that can be used in boosting the participation of diverse activities [19, 20]. Demonstrations also show that games give users an opportunity of interacting with an environment thereby simulating the real world. This has a positive influence on enjoyment, happiness, motivation, and pleasant mood, which in return increases the retention of knowledge and learning.

Therefore, this paper after critically reviewing the literature on cybersecurity gamification, alongside considering the theories and standard processes needed to develop a gamification tool that can incorporate cybersecurity concepts to boost knowledge of general cyber-users, proposes the design of a comprehensive cybersecurity gamification tool, a blend of both serious games and gamified elements to ensure the goal of the intervention is achieved in a balanced perspective. A survey is already prepared to test the validity of the intervention but will be presented in another publication as it's beyond the scope of this paper.

The remainder part of this paper discusses the methodology used in this design, results and discussions majoring on the promotion of cybersecurity knowledge via gamification, proposal of the design process and samples of the already developed gamification. Also, the paper concludes with an inclusive evaluation of the topic. This work aims at highlighting the role of gamification in promoting cybersecurity knowledge as well as indicate the standard design methodology for such special gamified systems, hence guiding interested scholars to design more inclusive and efficient cybersecurity interventions. Broadly, the results of the intervention can help mitigate the rate of cyberattacks on a global basis as well as provide a guideline for stakeholders and institutions to look towards designing more innovative interventions promoting cybersecurity knowledge and training.

II. METHODOLOGY

This paper employs an experimental design research approach, involving the practical theories and design steps needed for successful gamification of cybersecurity. Consequently, the design process alongside software used in developing the cybersecurity gamification intervention are presented in this section respectively.

A. Cybersecurity Gamification Theory

The current study is built on the Technology Threat Avoidance Theory (TTAT), as it gives explanations on the reason and manner in which users are able to avoid cyberthreats voluntarily [21]. TTAT was developed by

Liang and Xue to synthesize literature across diverse areas comprising psychology, health care, Internet security as well as risk analysis. Thus, its basic premise is that when a cyberthreat is being perceived by IT users, there is a motivation to avoid such threats actively via using certain safeguard measures if they perceive the avoidance of that threat by the prescribed measure of safeguard, after which they might as well avoid the threat passively via emotion focused coping performances.

First, users appraise the existence as well as the cyber threat level being faced and afterwards assess possible actions in avoiding such threats [22, 23]. Based on the appraisals, decisions are being made as to which measure of safeguarding could help in mitigating the threat faster. Several key factors are identified in reflecting user perceptions, motivations as well as behaviours during this process. In accordance with TTAT, a malicious threat would be avoided by users if they believe it is truly a threat and that it can be avoided via applying necessary safeguards. When being incorporated into a risk analysis research [24, 25] as well as health psychology [26], TTAT suggests that the determination of threat perception by users is via the threat occurrence perceived probability as well as the threat negative consequence perceived severity. Thus, being advised by previous health protective behaviour researches [27] as well as self-efficacy [28], there is a submission by TTAT, stating that users put three factors into consideration when evaluating the manner in which threat can be avoided, in the course of taking a measure of safeguard. These include: the safeguard effectiveness, safeguard costs, and the user self-efficacy in applying such safeguards.

B. Cybersecurity Gamification Design

In the process of gamification design aimed at education and training, there is a need for clarified definitions of specific training goals [29]. Moreover, in ensuring design of effective serious games, the selection of appropriate gamification elements that can suitably meet the needs of training approach is required [29]. As informed by literature, there are four gamification elements suggested for promoting cybersecurity knowledge, some of which are established for cybersecurity skills training. Progress mechanics: this relates to the motivation of players via providing progress tools such as badges, leader boards, and points. Player control: this refers to the use of a character (i.e., either 2D or 3D) which could engage in gamified training. Such character is usually referred to as an "avatar". From research, it has been discovered that behaviour can be influenced via the use of diversified role play of avatars. Problem solving: this refers to a vital gamification element which is incorporated if the goal of the intervention/training is to learn and retain novel information as the case is in this research where the goal is to promote cybersecurity knowledge. Thus, identification and collaboration of a collective resolution is of much importance in the development of strong problem-solving skills, which can be easily translated to practical knowledge at the end of the training/learning process. In some cases, a story is needed to ensure a proper flow of gamification. Story: this refers to a narrative that establishes a bonding effect/attachment between the avatar and learner respectively, and consequently creating a bond between participating avatars in a gamification-based training. It is important to state that learners are motivated by stories, as it keeps them playing and anxious to find out the remaining part of the story. Figure 1 illustrates the cybersecurity gamification design framework for this study.

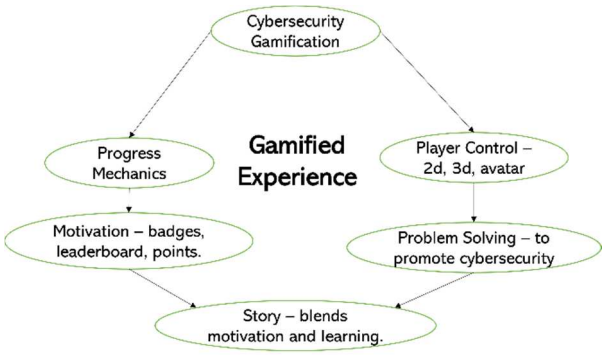

Figure 1: Cybersecurity Gamification Design Framework

C. Existing Solutions for Gamified Training

Contemporarily, several awareness interventions and cybersecurity trainings have introduced gamification techniques in their syllabus. Summarily, there are four aspects of gamifying cybersecurity as discovered in literature. Awareness: here, a minimum level of knowledge is required by participants, as it is majorly concerned about an entity's vulnerability level assessment, alongside providing the participants with general successful penetration attempt avoidance and detection knowledge. Defensive strategy: participants, who are most likely defenders, are required to possess substantial knowledge that will enable them to efficiently defend against cyberattacks with the appropriate tools and strategies. Offensive strategy: This positions participants in a rivalry to have a proper understanding of essential approaches and strategies. Attacker centricities: Here, the established characteristics of cyber-attackers are used in training users with the anticipation of the behaviour and motivation of an attacker to carry out specific tasks. Such anticipation augments the application and creation of both defensive and offensive strategies against cyber-attacks.

In this research, the proposed cybersecurity gamification employs the defensive strategy as the aim is to promote cybersecurity knowledge among general cybersecurity users to help them first understand different types of cyberthreats and how cyberattacks work. Moreover, gamification intervention is used to train participants, to maintain good cybersecurity behaviour as well as avoid social engineering scams. The target group are tertiary institution students from all levels; however, the gamification is designed to suit different target groups that fall within the general online users, thus providing some form of inclusiveness.

D. Software for Cybersecurity Gamification Development

There is several software suggested by literature that can be used to develop a cybersecurity gamification tool, the most preferred includes Unity 3D, Unreal Engine, and

Construct 3. After careful investigation of the pros and cons of the different game development engines, the Construct 3 game builder was chosen. The reason for choosing Construct 3 is due to its ease of functionality as well as its event-based visual scripting. Construct 3 was able to achieve the goal of the proposed ideation in developing the cybersecurity gamification prototype.

III. RESULTS AND DISCUSSION

In this section, the exact design process for the proposed cybersecurity gamification is presented. The chapter generally discussed about how cybersecurity knowledge can be promoted via proper design and implementation of gamification with a blend of serious games, where the focus is about knowledge immersion alongside certain enjoyment gamified elements, thus establishing an effective learning engagement among the participants.

A. Proposed Cybersecurity Gamification Concept

The cybersecurity gamification story is focused on contemporary cybersecurity issues, of which the player can relate with and thus, apply to avoid being vulnerable when faced with such realities. There are three levels in this cybersecurity gamification prototype. Each level focuses on a specific cybersecurity topic, with the aim of ensuring vast knowledge of cybersecurity is being imparted to the user. Level 1 is a mini game on social engineering. Level 2 is a mini-game on Network Security, while level 3 is a mini-game on Passwords. There is a section on Online security behaviours. The overall goal of this intervention is to ensure participants grasp adequate knowledge on prevailing cybersecurity issues and how to avoid or respond to cyberthreats. Moreover, there is a learn section, where general security tips are stored to enable participants to update their basic cybersecurity knowledge. As feedback is very important for this type of game, a feedback section was also included. This section directs the participants to a google form where they can answer a research survey about their cybersecurity knowledge, behaviour, and experience with the cybersecurity gamification tool they just played. The results of the feedback/surveys will be analysed statistically and used to develop a model which will be presented in a future publication. Figure 2 presents the home page of the proposed cybersecurity gamification prototype.

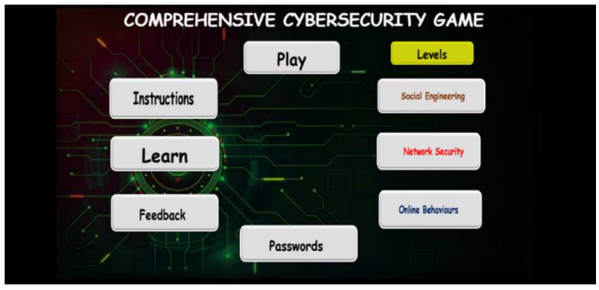

Figure 2: Home Page of the Comprehensive Cybersecurity Gamification

B. Cybersecurity Gamification Levels Gameplay

As mentioned earlier, there are 3 levels in the cybersecurity gamification proposed by this research. There are different types of gameplays for the 3 levels to promote cybersecurity knowledge in the various security topics. They are discussed thus:

1. Level 1: Social Engineering Mini-Game

Contemporary networks have experienced a rapid increase in the attacks caused by social engineering, thereby weakening the cybersecurity chain. The aim of social engineering attacks is to manipulate individuals and organizations to disclose sensitive and valuable data that can be of interest to cyber attackers [30]. Therefore, social engineering is a great challenge to both human and computerized networks.

The social engineering game style was designed like a platformer game where a player can move, run, jump around a platform. In this game, social engineering was illustrated via game objects that represented security vulnerabilities. Some of these objects included compromised flash drives, phishing emails, fake calls (vishing), fake social media news, among others. The idea is for the player to try to avoid these flashy yet compromised objects during gameplay. If they interact with the compromised objects, they will lose points and a security warning will pop up concerning the specific social engineering enemy they interacted with, and the game will restart. Furthermore, there are other game elements in the social engineering game, which includes safeguard measures, expected of the player to interact with to gain points. Apart from gaining points, if a player interacts with the safeguard measure objects, varieties of cybersecurity tips to avoid social engineering scams will pop up for the player. This way, the player can gain some extensive knowledge about social engineering scams and how to avoid them, while at the same time enjoying the game. The score points are motivations for the player to keep playing the game, while learning more cybersecurity tips on social engineering. Figure 3 depicts the social engineering game level.

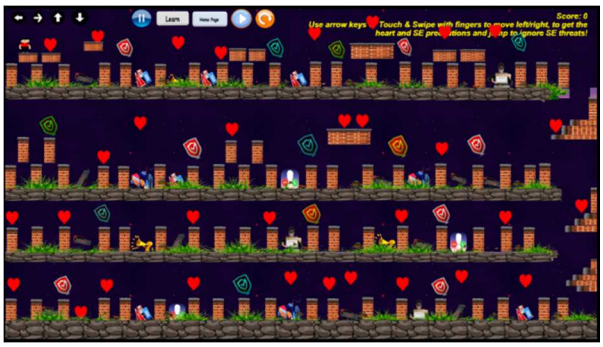

Figure 3: Social Engineering Game Level

2. Level 2: Network Security Mini-Game

For the network security level, the game is designed in such a way that players can understand network security threats, as well as have a feeling of how to defend themselves to avoid been attacked by network attackers. To give a proper and realistic gaming experience, a shooting game was used for the network security level. The players

are in a real war game, where game objects representing various network threats, such as malware, viruses, trojan horse, DDOS, ransomware scams span towards the player's direction to attack. The player is a 2D character that can shoot and fire the enemies as they come towards them. To ensure the goal of imparting cybersecurity knowledge is achieved, several definitions and security tips on network attacks (which can be understood by a novice) keep popping up the screen in interval of 15 seconds during gameplay. This way, the player while trying to defend themselves from being killed by the network security attacks, also learns about these threats and how to avoid them in a real security encounter. If the player successfully shoots the network security enemy, they will score 50 points, this motivates the player to keep shooting the enemy and keep learning more of the network security safeguard tips popping up during the game play. The feeling is immersive, and the game is engaging enough to achieve the goal of educating the participants on cybersecurity. However, if the player collides with the enemy object, they get killed and loose points, and the game restarts again. Figure 4 illustrates the network security game level.

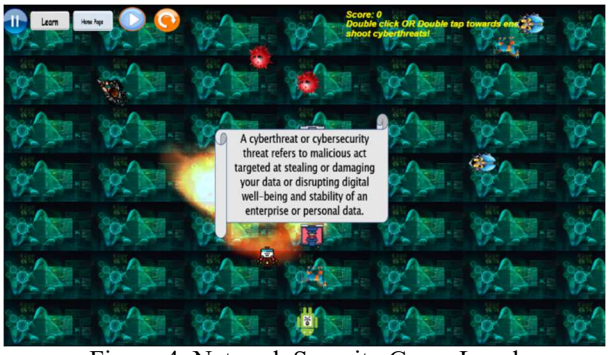

Figure 4: Network Security Game Level

3. *Level 3: Password Security Mini-Game*

For the password security game level, the goal is to teach participants how to detect weak passwords and avoid them, as well as proper way of choosing a strong password for their online accounts. This game is quite simple, as the goal is not to present a very complex system but propose an intervention that can help in improving the knowledge of users on various cybersecurity issues. In this game, strong and weak passwords are created as game objects which can display the passwords for the player to see and choose. If the player chooses a weak password, they will lose points and be cautioned of the danger of using a weak password for their online accounts, after which the game will be over and restart. However, if they choose a strong password, they will gain points, and be reminded of the importance of using a strong password as well as tips of good password security management, such as regular changing of passwords, not storing passwords in unsafe locations either on mobile device or laptop. The overall goal of the game is to teach the users on proper security measures to enable them to maintain good cybersecurity assurance. Figure 5 illustrates the password security game level.

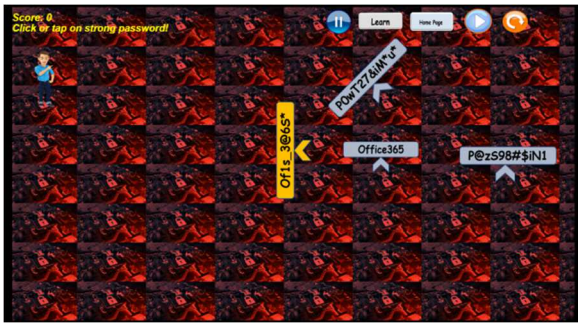

Figure 5: Password Security Game Level

C. *Promoting Cybersecurity Knowledge via Gamification*

From the proposed intervention, the goal of the gamification is not just for entertainment or fun, but to engage the participants to learn about cybersecurity and gain substantial knowledge that can help in being aware and defend against cyberthreats. Moreover, as literature has established, gamification can be used in cybersecurity training programs, though most publications are still focusing on the ideation phase. There is less publicity on actual development of interventions that promote cybersecurity knowledge via gamification as proposed in this chapter. Recently, a study by Ros, et al. [31], analysed students' self-perception of success and learning effectiveness via gamification in an online cybersecurity course based on cognitive constructivism learning theory. Though, an interesting game, however, it was narrowed down to just computer science students in a cybersecurity course, a trend practiced by most related studies [32, 33]. There is a need for more inclusive cybersecurity games that can cover various aspects of cybersecurity and are designed in a simplistic approach so that the general audience can understand the basic cybersecurity concept. Thence, this comprehensive cybersecurity game can address 3 major aspects of cybersecurity as well as balance learning and enjoyment in a motivative manner.

Cybersecurity refers to a global multifaceted phenomenon in which the commercial sector alongside governments is presented with socio-technical issues of much complexity. Due to the evolvement of technology, various volumes, and type of cyberattacks poses diverse effects on several users via spectacular approaches. However, human errors are the major causes of majority of cyberattacks. Regardless of the environmental as well as knowledge dependency of cyberattacks vulnerability by humans, there are suggestions from research regarding improvement of cybersecurity awareness as well as knowledge promotion. This, if implemented appropriately will be among the best measures of prevention. Nevertheless, due to end-user's character intangibility, socio-technical interdependency, indistinct impact, and continuous evolution of technology, fighting cyberattacks as well as proposing more inclusive communicative techniques becomes challenging. Thus, the essentiality of equipping individuals at prime age with adequate cybersecurity knowledge and skills that can help combat cyberthreats cannot be overemphasised.

Gamification has been proven to boost involvement of students as well as increase their interest in study. Via a training program tailored towards gamification, constituent of a game is used in providing scenario of work in reality/realism [19, 33]. Thence, the essence of designing training programs based on gamification is first to achieve set goals of an institution via strategic objective alignment. Based on research findings, training programs that are gamified afford participants a learning environment distinct enough to enhance attention of the learners as well as increase information engagement [20, 34]. Moreover, on the side of the developers, series of attributes for training purposes are being considered in the game, some of which includes, badges, group competition, leader boards, feedback, points, challenges, social points, storytelling, achievements, levels, likes, and incentives, respectively. All this is used in encouraging participants to oversee achieving the targeted goals. As informed by literature, the prevalent game-like elements used in most gamified training programs comprise challenges, scores, ranking, points, and leader boards.

Being a novel profession, cybersecurity education faces a lot of impediments, yet continuously witnesses a growing demand. The future of cybersecurity training is brighter as gamification and serious games have more potential to expatiate adequate knowledge of cybersecurity in an outstanding manner. However, there are concerns that need to be addressed as concern the lack of standardized design techniques and methodologies for cybersecurity gamification because of the unfathomableness of game-inclined learning approach. Moreover, the escalating rate of cyberattacks is triggered by lack of knowledge and awareness of insecure online behaviours among end-users, such as ignoring security warning alerts. Interacting with unauthentic information sources and surfing vulnerable webpages. Thus, gamification via serious game implementation has potential of improving conceptual assimilation alongside cognitive development, yet there is scarcity of mobile games or gamification interventions that is focused on educating cyber-users about cybercrimes and its preventive measures.

IV. CONCLUSION

A. Study Limitations & Future Work

The current achievement is an inspiration for future researchers to come up with more comprehensive innovations of integrating gamification to promote cybersecurity knowledge via emerging technologies such as AI, Deep learning, machine learning, robotics, etc. with the aim of improving the effectiveness of the intervention. Furthermore, future cybersecurity gamifications should focus on explicitness of experiential goals and objectives as well as provide an effective follow-up technique to participants to ensure the identification of lasting impacts and retention. Though there is some form of popularity among serious games, there is serious need for further investigations that can proffer assurance of their efficiency as well as aid comprehension of vital subjects by end-users. Cybersecurity gamification should include realistic and naturalistic disaster in its training intervention. Due to the wide range of digital cybersecurity games alongside variance in platforms, it is imperative for game makers to focus on the aspects of cyber safety instead of gamification, hence ensuring the goal of gamification in the first place is not underachieved. Apparently, the current scope of games application in cybersecurity training and awareness gives room for in-depth interaction of cybersecurity content themes in a conducive environment, with the major goal of expanding participation of cybersecurity and the long-term goal of establishing cybersecurity assurance across the globe.

B. Contributions

Cybersecurity is now contemporarily a challenging interesting research area that keeps evolving as a major issue globally. This is due to the rapid level of cyber-attacks, leaving a lot of companies and individuals at high risk of victimisation. This paper presented the design of an innovative intervention via gamification to promote cybersecurity knowledge among general Internet users. The comprehensive cybersecurity gamification, which comprises three levels, social engineering, network security, and password security, provides an inclusive motivational learning engagement for participants to equip themselves with substantive cybersecurity knowledge. This will help participants be first aware of the existing cyber threats, how to face and respond to prevailing cyber-attacks, and determine how to maintain good cybersecurity behaviours that can help ensure fantastic cybersecurity assurance in society. Future work is ongoing by the researchers to test the cybersecurity gamification and propose a cybersecurity knowledge behavioural model which will serve as a guide for researchers and stakeholders to build more accelerated interventions to promote cybersecurity awareness and knowledge respectively.

C. Conclusion

Incorporation of game elements in the field of Information Communication Technology in general have proven to be an engaging tool for learners [35]. Moreover, in cybersecurity training, numerous studies have shown that gamification is a viable medium of fostering engagement among employees. Numerous end-users from various fields have expressed satisfaction and enjoyment of gamification in addressing different issues. Moreover, there is a need to include the privacy aspect of gamification during the development stage as individual traits and confidential information are being recorded on game play. A couple of techniques examine requirements for privacy and security, however, only a few ends up integrating gamification. Gamification increases engagement in educational training. Awareness of privacy is achievable via building gamification interventions that can educate end-users on privacy safeguards techniques.

ACKNOWLEDGMENT

The authors would like to thank Universiti Kuala Lumpur, Malaysia for funding this research under the

UniKL Excellent Research Grant Scheme (UERGS) ref no: UniKL/CoRI/UER22008.

REFERENCES

[1] Z. Yan *et al.*, "Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?," *Computers in Human Behavior,* vol. 84, pp. 375-382, 2018.

[2] T. van Steen and J. R. Deeleman, "Successful gamification of cybersecurity training," *Cyberpsychology, Behavior, and Social Networking,* vol. 24, no. 9, pp. 593-598, 2021.

[3] R. Matovu, J. C. Nwokeji, T. Holmes, and T. Rahman, "Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges," in *2022 IEEE Frontiers in Education Conference (FIE)*, 2022: IEEE, pp. 1-9.

[4] M. Malone, Y. Wang, K. James, M. Anderegg, J. Werner, and F. Monrose, "To gamify or not? on leaderboard effects, student engagement and learning outcomes in a cybersecurity intervention," in *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education*, 2021, pp. 1135-1141.

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

[6] T. Sawik, "A linear model for optimal cybersecurity investment in Industry 4.0 supply chains," *International Journal of Production Research,* vol. 60, no. 4, pp. 1368-1385, 2022.

[7] B. D. Sawyer and P. A. Hancock, "Hacking the Human: The Prevalence Paradox in Cybersecurity," *Human Factors,* vol. 60, no. 5, pp. 597-609, 2018, doi: 10.1177/0018720818780472.

[8] B. F. Faith, Z. A. Long, S. Hamid, O. F. Johnson, C. I. Eke, and A. Norman, "An Intelligent Gamification Tool to Boost Young Kids Cybersecurity Knowledge on FB Messenger," in *2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, 3-5 Jan. 2022 2022, pp. 1-8, doi: 10.1109/IMCOM53663.2022.9721733.

[9] N. Coull *et al.*, "The gamification of cybersecurity training," in *International conference on technologies for E-Learning and digital entertainment*, 2017: Springer, pp. 108-111.

[10] C. C. Taladriz, "Flipped mastery and gamification to teach Computer networks in a Cybersecurity Engineering Degree during COVID-19," in *2021 IEEE Global Engineering Education Conference (EDUCON)*, 2021: IEEE, pp. 1624-1629.

[11] S. Scholefield and L. A. Shepherd, "Gamification techniques for raising cyber security awareness," in *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21*, 2019: Springer, pp. 191-203.

[12] K. H. Sharif and S. Y. Ameen, "A review of security awareness approaches with special emphasis on gamification," in *2020 International Conference on Advanced Science and Engineering (ICOASE)*, 2020: IEEE, pp. 151-156.

[13] S. O'Connor *et al.*, "SCIPS: A serious game using a guidance mechanic to scaffold effective training for cyber security," *Information Sciences,* vol. 580, pp. 524-540, 2021/11/01/ 2021, doi: https://doi.org/10.1016/j.ins.2021.08.098.

[14] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A Serious Game for Cyber Security Awareness and Education," *Computers & Security,* vol. 95, p. 101827, 2020/08/01/ 2020, doi: https://doi.org/10.1016/j.cose.2020.101827.

[15] M. M. Yamin, B. Katt, and M. Nowostawski, "Serious games as a tool to model attack and defense scenarios for cyber-security exercises," *Computers & Security,* vol. 110, p. 102450, 2021/11/01/ 2021, doi: https://doi.org/10.1016/j.cose.2021.102450.

[16] A. Abd-Alrazaq *et al.*, "The effectiveness and safety of serious games for improving cognitive abilities among elderly people with cognitive impairment: systematic review and meta-analysis," *JMIR serious games,* vol. 10, no. 1, p. e34592, 2022.

[17] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, "Cybersecurity knowledge and skills taught in capture the flag challenges," *Computers & Security,* vol. 102, p. 102154, 2021/03/01/ 2021, doi: https://doi.org/10.1016/j.cose.2020.102154.

[18] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Computers in Human Behavior,* vol. 48, pp. 51-61, 2015.

[19] S. Das, "SoK: A Proposal for Incorporating Accessible Gamified Cybersecurity Awareness Training Informed by a Systematic Literature Review," in *Proceedings of the Workshop on Usable Security and Privacy (USEC)*, 2022.

[20] Z. Batzos *et al.*, "Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview," 2023.

[21] H. Liang and Y. L. Xue, "Understanding security behaviors in personal computer usage: A threat avoidance perspective," *Journal of the association for information systems,* vol. 11, no. 7, p. 1, 2010.

[22] R. Bitton, A. Finkelshtein, L. Sidi, R. Puzis, L. Rokach, and A. Shabtai, "Taxonomy of mobile users' security awareness," *Computers & Security,* vol. 73, pp. 266-293, 2018.

[23] W. Li, T. Yigitcanlar, I. Erol, and A. Liu, "Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework," *Energy Research & Social Science,* vol. 80, p. 102211, 2021/10/01/ 2021, doi: https://doi.org/10.1016/j.erss.2021.102211.

[24] F. Liebana-Cabanillas, F. Munoz-Leiva, and J. Sanchez-Fernandez, "A global approach to the

analysis of user behavior in mobile payment systems in the new electronic environment," *Service Business,* vol. 12, no. 1, pp. 25-64, Mar 2018, doi: 10.1007/s11628-017-0336-7.

[25] P. van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev, "Risk perceptions of cyber-security and precautionary behaviour," *Computers in Human Behavior,* vol. 75, pp. 547-559, Oct 2017, doi: 10.1016/j.chb.2017.05.038.

[26] D. Vollmer Dahlke and M. Ory, "mHealth applications use and potential for older adults," *Encyclopedia Geropsychology,* pp. 1-9, 2015.

[27] D. King, F. Greaves, C. Exeter, and A. Darzi, "'Gamification': Influencing health behaviours with games," *Journal of the Royal Society of Medicine,* vol. 106, no. 3, pp. 76-78, 2013, doi: 10.1177/0141076813480996.

[28] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of Experimental Social Psychology,* Article vol. 19, no. 5, pp. 469-479, 1983, doi: 10.1016/0022-1031(83)90023-9.

[29] B. Caulkins, T. Marlowe, and A. Reardon. *Cybersecurity Skills to Address Today's Threats, Advances in Intelligent Systems and Computing*, vol. 782, pp. 187-192, 2019.

[30] J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept," *Computers & Security,* vol. 73, pp. 102-113, 2018.

[31] S. Ros, S. González, A. Robles, L. Tobarra, A. Caminero, and J. Cano, "Analyzing Students' Self-Perception of Success and Learning Effectiveness Using Gamification in an Online Cybersecurity Course," *IEEE Access,* vol. 8, pp. 97718-97728, 2020, doi: 10.1109/ACCESS.2020.2996361.

[32] A. Mittal, M. P. Gupta, M. Chaturvedi, S. R. Chansarkar, and S. Gupta, "Cybersecurity Enhancement through Blockchain Training (CEBT) – A serious game approach," *International Journal of Information Management Data Insights,* vol. 1, no. 1, p. 100001, 2021/04/01/ 2021, doi: https://doi.org/10.1016/j.jjimei.2020.100001.

[33] C. DeCusatis *et al.*, "A Cybersecurity Awareness Escape Room using Gamification Design Principles," in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 26-29 Jan. 2022 2022, pp. 0765-0770, doi: 10.1109/CCWC54503.2022.9720748.

[34] H. Gonzalez, R. Llamas, and F. Ordaz, "Cybersecurity Teaching through Gamification: Aligning Training Resources to our Syllabus," *Research in Computing Science,* vol. 146, pp. 35-43, 2017.

[35] J. Krath, L. Schürmann, and H. F. O. von Korflesch, "Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning," *Computers in Human Behavior,* vol. 125, p. 106963, 2021/12/01/ 2021, doi: https://doi.org/10.1016/j.chb.2021.106963.