Atlantis Highlights in Computer Sciences, volume 4
Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)

Cybersecurity Awareness Among the Youngs in Malaysia by Gamification

Ng Jia Jian[1,*] Intan Farahana Binti Kamsin[2]

[1, 2]*Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia.*

**Corresponding author. Email: tp054641@mail.apu.edu.my*

ABSTRACT

Cybersecurity is getting more critical and important to the digital world nowadays. Government, military, company, and medical industry use technologies to collect and store sensitive data and information for many purposes. There are more cybercrime cases raise at the same time. The reason is that people are still lack of cybersecurity awareness especially the Youngs age between 13 years old to 15 years old. The aim of this research is to study on how to increase cybersecurity awareness among teenagers by using gamification, and how a computer game would attract teenagers to learn about cybersecurity. At the end of this research, a computer game named “BEWARE” is developed to achieve the aim. For this research, quota sampling method is applied to 50 secondary students range age from 13-15 years old in Malaysia by using Online survey. 3 students were randomly selected to participate in the interview session to ensure the online survey result is reliable. An area of future research to raise the awareness of cybersecurity that would be recommended that is focusing more on actions must take by schools and find out more interesting way to help the Youngs to notice about cybersecurity.

Keywords: *Cyberattack, Cybersecurity, Cybersecurity awareness, Cybersecurity Computer Game, Gamification.*

1. INTRODUCTION

This proposal is about increase cybersecurity awareness level among the Youngs by developing a cybersecurity computer game. Nowadays, human life has been serving well by the numerous benefits of the rapid changes in technology. However, it also raises the rate of cybercrime at the same time. According to the survey result of a target group of secondary students aged 13-17 years, 80% of them uses internet at least 2-3 days a week, 92.47% of them have social media accounts, 77% of them seldom change their password [17] [33-36]. Based on that result, it can be concluded that the students are highly exposed to the internet. According to Asokhia [8], young generation has the high risk of becoming the victim of cybercrime and thus they need to be protected. Nurul ‘Ain Ahmad and Nooraini Othman [2] stated that the number of cases such as internet scams, cyberbullying, online harassment, identity fraud, and so on are increasing day by day due to the lack of awareness on the knowledge of Internet [39, 40]. They also stated that based on the statistics, the most common age of victims who are easy to become a target is from 13 years old to 15 years old. This is because the Youngs are unaware of the consequence and impact of revealing their personal information [1]. It is necessary to educate the Youngs on the best practices and how to behave on the internet.

The objectives of this research are:

1. To build a computer game to inspire young people interest in learning.
2. To implement simulation element which users are training in a simulated real-world environment for better learning process.

3. To enhance users learning performance by adding leadership board feature for scoring competition.

Therefore, a cybersecurity game is being proposed in this paper to educate the Youngs on the cybersecurity knowledge. This game will implement simulation element that the Youngs will be trained in a simulated real-world environment and taught how to effectively react to a specific situation relate to cybersecurity threats that they may be faced in real world. The real-world environment is simulated on first person mode which is entirely different from others cybersecurity game. It enables the Youngs to learn cybersecurity knowledge in an interesting way that allow the players to make themselves greatly involve in the situations. It is easier for the players to remember what they have been practicing in the game, effective learning achieved. They can always get second chance to correct their mistake in simulated environment which is impossible in the real-world. In order to ensure the players are familiarized with the recent techniques used in the real world, the players are given scenarios which are designed based on recent techniques used by the scammers in real world. Besides, the proposed system is implemented leadership board feature that has not been built in the similar systems. Leadership board feature allows the Youngs to have scoring competition in order to stimulate their learning performance. Schools can give attractive rewards to the students based on their ranking in leadership board, therefore this encourages students to compete with each other to strike for the rewards and thus improve their cybersecurity knowledge.

2. RELATED WORK

2.1 Cybersecurity

The meaning behind the term Cybersecurity is about defending digital system and assets from online illegal activities [9] [37, 38]. In other words, it is means that protecting and preventing data fall under bad people hands for criminal purposes [29-32]. This term has also been defined by several researchers. Cybersecurity is about technologies, processes, and practices to against the attack, damage or unauthorized access on the networks, data, and computers [10]. According to Lene Hansen and Helen Nissenbaum [23], the concept of cybersecurity is indicating a lack of security in computer networks in early 1990s. However, recently this concept is more than mere insecurity and has then become a real problem requires attention and appropriate solutions to protect internet users from cyber threats [13]. The problem related to cyber threats is important and should be taken into account early before it does serious impact to the internet users especially young users [24]. For instance, the problem bought by the growing of internet can be pornography that can lead to social problem including crime [25].

2.2 Cybersecurity awareness in Malaysia

Cybersecurity awareness can be defined as the user's level of awareness of the online best practice [15]. D.S. Cruzes el at [26] also defined cybersecurity awareness as a form of education that give cybersecurity knowledge to the internet users to be alert to the various cyber threats and vulnerability of IT assets to these threats. Malaysian Communications and Multimedia Commission (MCMC) has reported that an average of 6.6 hours online spent daily in 2018. This may be a risk to become a victim of cybercrime as the longer they stay online, the higher the risk. Adamu Abdullahi Garba et al [27] mentioned that there is a greater risk for the young and immature students whose often look for the information via improper online conduct to satisfy their curiosity. Nurul 'Ain Ahmad and Nooraini Othman [2] also stated that the Youngs in age 13-15 years are the common group of people to become an easy target as they are unaware of cybersecurity. However, based on the survey result by Zulkifli et al [16], 86% as the majority of secondary school students in Malaysia are willing to learn about cybersecurity awareness. This indicates a good sign to develop a best solution to educate them on cybersecurity awareness. When comes to responsibility, 55% of the students think government must endorse cybersecurity awareness, while other 33% think that it is the responsibility of parents for cyber safety [16]. Education in cybersecurity awareness is not only essential for primary and secondary students, but every level of students. In Malaysia, although "CyberSafe" by Cybersecurity Malaysia that works to spread the awareness of cybersecurity especially to the kids, youth, and parents, it is not reachable enough to educate them all.

2.3 Gamification

The term of gamification has no final definition on its [12]. But this term has been defined by some research studies regarding the contexts in which it is applied. In other words, gamification can be known as application of game design in non-gaming contexts to motivate and influence people [12]. These contexts can be in health, education, marketing, and finance. In addition, gamification can be also defined as a methodology of designing and creating systems that give similar experiences and motivations when playing games and include educational goal of influencing user behavior [11]. There are two concepts that are closely related to Gamification are serious game and game-based learning [28]. Game-based learning refers to the game that designed for the intention of educating while entertaining by including problem-solving and challenges that provide players sense of achievement [28]. According to Prensky, digital game-based learning is a new feature that is capable to deliver education materials via interesting games while enjoying at the same time [18]. While serious games are designed for the serious purpose which beyond education. Common example is the training or simulation in the industries such as military, health, science, and even politics, that is rather focusing on training than entertainment [18], [28]. The concept of gamification started to attract people attention around 2010 [14]. By gamifying the contexts, people can practice their behavior and skills without stress in a safe environment. Leaderboards, points, quest/mission, medals, and feedback are the key gamification mechanism suggested by several research of application of gamification concept [3]. By concluding the previous definitions mentioned, gamification is usually implemented to increase engagement and motivation of people. Research studied on gamifying laboratory experience by Drace [19] has proved that the gamified skills and materials from the lecture made the students felt engaged and interested.

2.4 Cybersecurity awareness by gamification

Human factor is the weakest link in cybersecurity. In other words, people are vulnerable to the cyber threats as lacking cybersecurity awareness, like downloading untrusted files, opening attachment without checking, and sharing sensitive documents that they created opportunities for the perpetrators [7]. Cybersecurity awareness must be spread around people. Cybersecurity awareness is not an easy task. It needs people’s understanding, differentiation, and application of the concept that are commonly scarce. An excellent example to achieve the requirements is gamification that is an approach of using digital and non-digital games in non-entertainment context to fulfill the objectives [20]. Gamifying cybersecurity knowledge has more potentials to help students to have better understanding on the complex and unfamiliar concepts in cybersecurity [21]. There are several cybersecurity-based games have been established to educate, especially children, and young people. An example of the game is Cybersecurity Lab that is designed to educate young people basic cybersecurity skills.

2.5 Systematic Review

2.5.1 Overview Proposed System

***BEWARE**, the cybersecurity game.*

BEWARE is a simple computer game that is covering the aspects of cybersecurity in the gameplay. These aspects can be information security, social engineering, email phishing, identity fraud, and more. It is a role-play game that the players control a fictional character to do mission, and tasks in an imaginary world. The game environment is simulating a real-world environment with a basic but interactive graphic that can give players a great gaming experience.

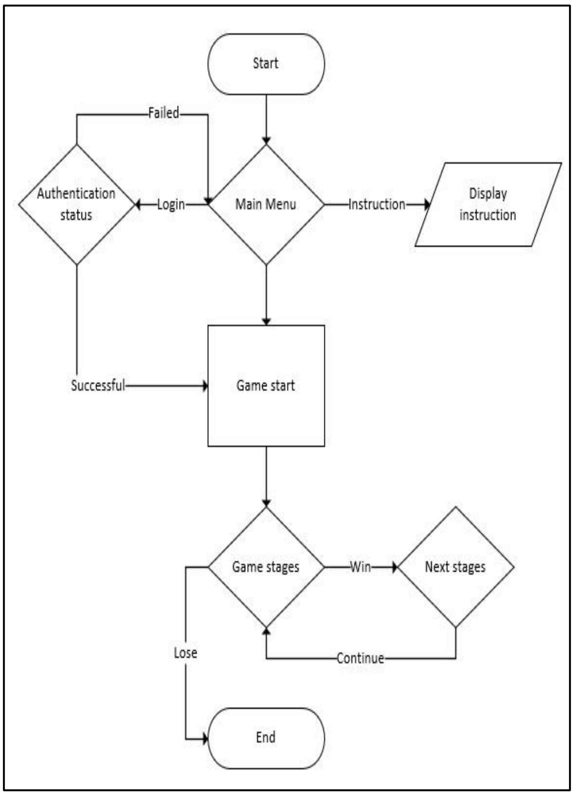


Figure 1 Flowchart of the overview system

Figure 1 shows a flowchart of the overview of system. The game is going stage by stage. There is different type of game mode in BEWARE. The game mode will be different in every stage. The players may be asked to make decision on a scenario provided by the NPC or do the mission/tasks within time given. Mission failure and wrong decision made will lead to reduce point. However, there are some circumstances in which the failure of the mission will trigger a “fatal” penalty that will cause the player to lose in-game. There will be some quiz to be answered in between the stages. Points will be awarded to players if the answer is correct. In addition, there is a leadership board feature to record all the high scores of players.

Considering most the Youngs are immature in decision making, especially when they do not aware of the cybersecurity. Thus, they need to be educated. By using decision making mode, the player can learn how to response to the circumstances if it is in real-world. In decision making mode, NPC will provide a scenario to the player. The player should select one of the decisions among the given options. As mentioned above, the wrong decision made will lead to lose in game or loss in points. For instance, an NPC from the bank will ask the player to provide his bank information such as PIN or password for verifying purpose. In this case, the player will have to select a decision whether give or do not give. After decision has made, the correct answer will be displayed with explanation, and point will be given. Therefore, the players can see what the consequence of their choices is and learn from it.

Besides, some stages are required the players to do some quests. These quests must be done within the time given. The longer the time taken, the lesser the point given. One example of the quest in this game is that the player must point out the things which must be paid attention to in an email to avoid email phishing. The knowledge for this quest was provided through the conversation between the player and the NPC. So, the player must pay attention to what NPC said before.

2.5.2 Similar systems

2.5.2.1 Hot Spot

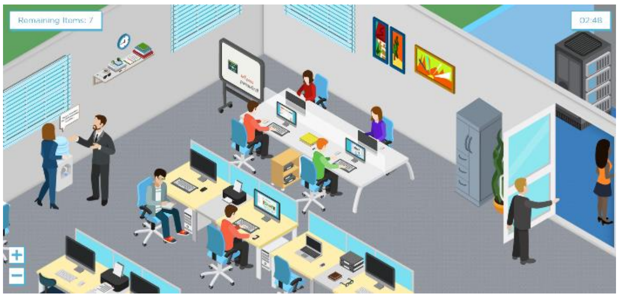
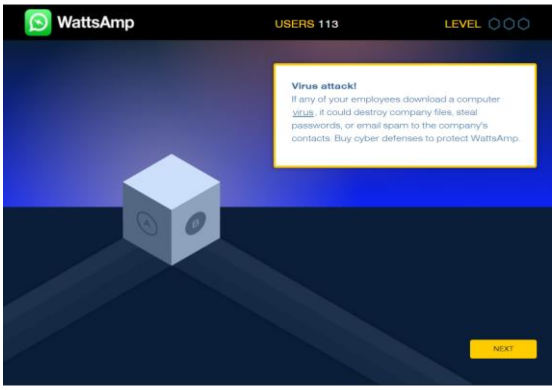


Figure 2 HotSpot in game

Hot spot is one of the cybersecurity games in education context. The game is running in a simulation of work environment. This game contains very basic knowledge of cybersecurity related to office environment. User is asked to find out the violations that scattered around by clicking on the items before the time runs out. Once the user spotted the violation, a message will pop-up that provides security knowledge to the user related to the specific violation. There is no limit of tries.

2.5.2.2 Cybersecurity Lab

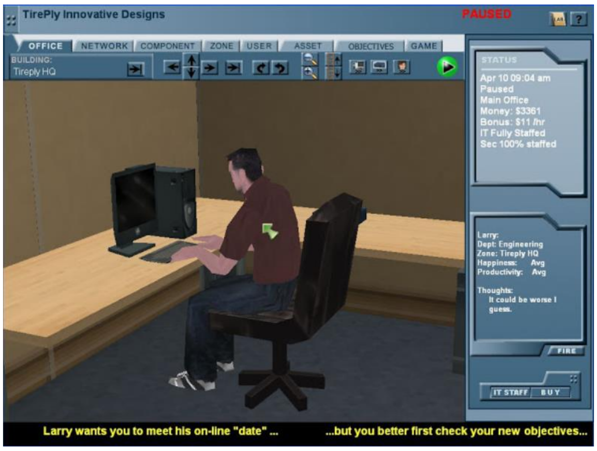


Virus attack!
If any of your employees download a computer virus, it could destroy company files, steal passwords, or email spam to the company's contacts. Buy cyber defenses to protect WattsAmp.

Figure 3 Cybersecurity Lab in game

Another cybersecurity game is Cybersecurity Lab from NOVA Labs website. Cybersecurity Lab is challenging users to play a role of chief technology officer of start-up social media company against increasingly gradual attacks. The goal is to enhance cyber defenses by winning a number of challenges. There are four main challenges in this game such as Coding, Password-Cracking, Social Engineering, and various of cyber battles. This game has real-world stories of cyber-attacks animated in videos that explain the need for cybersecurity.

2.5.2.3 CyberCIEGE



BUILDING: Tireply HQ

Apr 10 09:04 am
Paused
Main Office
Money: $3361
Bonus: $11 /hr
IT Fully Staffed
Sec 100% staffed

Larry:
Dept: Engineering
Zone: Tireply HQ
Happiness: Avg
Productivity: Avg
Thoughts:
It could be worse I guess.

Larry wants you to meet his on-line "date" ... ...but you better first check your new objectives...

Figure 4 CyberCIEGE in game

CyberCIEGE is a serious cybersecurity game designed mainly for employees to have lesson on network security concepts. This game required basic knowledge on network security. It has an interactive environment. The players spend virtual money to defend their network by purchasing and configuring workstations, servers, network devices, and operating systems. The game is challenging users to maintain a balance between budget, productivity, and most importantly optimizing security by making tradeoffs. The players can see the consequences of their selections

Table 1. Comparison table of CyberCIEGE, Cybersecurity Lab, Hot Spot, and Proposed system

System / **Criteria**	**CyberCIEGE**	**Cybersecurity Lab**	**Hot Spot**	**BEWARE (Propose system)**
Leadership board	No	No	No	Yes
Overall Graphic	Low	Low	Low	Medium
Simulation	Yes	Yes	Yes	Yes
User type	Employee	Young	Employee	Young, Employee
Basic knowledge requires	Yes	No	No	No

Based on the system analysis, only BEWARE implementing leadership board feature. This feature stimulates participant's motivation on learning by having competition with their friends or colleagues. Besides, BEWARE has better graphic for a better visualization compared to the other similar systems. An awesome graphic is capable to attract people to get interested to play the game. All systems do have simulation. However, BEWARE has "First person" mode in simulation which is different from the other three systems. First person mode enables player to fully involve in the game situations. This proposed system is suitable for Youngs and even employees compared to other three systems which can only be suitable for single user type. CyberCIEGE is suitable for training and taking course. For Hot Spot, there is only office/workstation environment in the game which the information is insufficient to educate Youngs. Moreover, there is no foundation of cybersecurity required in BEWARE and the other two systems except for CyberCIEGE. This is because CyberCIEGE is a serious game which is focus on education rather than entertainment, so it does need basic security knowledge to play.

3. METHOD

Research methodology is a process of collecting, processing, categorizing, and analyzing the data for a particular topic by using methods and techniques. This part is essential for every research because it allow the researchers to ensure their aim and objectives are supported by valid and reliable results. For this research, online survey with quota sampling method is applied to 50 secondary students range age from 13-15 years old in Malaysia. In addition, qualitative research is executed to 3 students were randomly selected to participate in the interview session. This is to ensure the online survey result is accurate and reliable.

3.1 Sampling Method

Quota sampling method is a non-probability sampling technique in which the participants were selected according to specific traits or qualities determined by the researchers [4]. The selected sample would then represent a population. In this research, a subgroup of age range 13-15 years old teenager is the targeted group to find out their awareness level on cybersecurity. Therefore, quota sampling method is used as it is a suitable method to locate a subgroup of people that would have a great contribution to the research.

3.2 Online survey

Survey method can be understood as collecting data by questioning individuals relate to the topic. This method can obtain valuable and reliable data from the large group of people in no time. As mentioned above, survey method is used in this research. The survey is Likert scale-based with several closed-ended and open-ended questions by using Google form. The reason of applying Likert scale-based survey is that it is a reliable way to measure opinions and perceptions as well as person ability estimates [5]. Meaning that the participants can specify their level of cybersecurity awareness. In addition, considering the less of time, using Likert scale-based survey is better because it allows the researchers to collect data from many respondents rapidly [5]. Besides, closed-ended questions are often good for survey due to very straight forward questions. To obtain the data in more detail, open-ended question is included to give a free form answer. There will be 50 secondary students age from 13-15 years old in Malaysia participating in this research.

3.3 Interview

Interview is one of the effective data collection methods that is to ask the participants several questions face-to-face. There are three type of interviews such as semi-structured, structured, and unstructured. In this research, one-to-one structured interview is used in which the participants are questioned by a list of predetermined questions [6]. 3 respondents are chosen randomly to have interview session. The reason for this research to carry out interview in structured way is that time will be saved as the questions are prepared in advanced to reduce mistakes during interview. In addition, according to Anja, the Content Marketing specialist, structured interview is easy to compare the answers from respondents because they are asked on the same questions. Thus, the results are easier to be analyzed compared to unstructured interview. While unstructured interview is an approach that does not prepare question in advanced and with little or no organization for the flow of event [6] Thus, it may lead to failure. As mentioned above, the purpose of conducting interview not only to gather data but to ensure the accuracy of the survey results.

4. DISCUSSION

Cybercrime is increasing in Malaysia due to the lack of awareness of cybersecurity threats among teenagers age between 13-15 years old. These cybersecurity threats can bring serious impact to the young generations such as financial loss, cyberbullies, damage in asset, identity fraud, and so on. It is essential to increase the teenager’s cybersecurity awareness which is the most critical part of this research. Upon considering the young’s hobby-interested in game, deliver the cybersecurity materials through a game is an ideal solution to raise the cybersecurity awareness among the Youngs. They will get motivated to fully engaged in the educational process by the interactive game if there are rewards and objectives established [22]. A computer game named “BEWARE” will be developed with an attractive graphic, leadership board feature, and simulation element that would greatly inspire the Youngs to effectively increase their awareness of cybersecurity in a much interesting way. In the game, the players, as well the Youngs, are given scenarios that were happened in real life to answer. This game will prepare them on how to react these threats in real-world. They can always practice their mistakes in the game. Thus, playing this game, they can get themselves familiarize with the threats and has the ability to response to it in a quick and proper way before they encounter it in their daily life which would not give second chance for them to react. There are several similar games related to cybersecurity on the internet. However, simulation element and leadership board feature which are implemented in the computer game is less to be seen in those other similar games.

5. CONCLUSION

Overall, as mentioned above, the Youngs are easy target to the perpetrators. It is necessary to increase the cybersecurity awareness among them early before the threats cause serious impact on them. In addition, they should be educated regularly on Cybersecurity awareness as there will always new threats developed in the future. Through this game, Youngs will be educated with the knowledge of how to protect themselves from cybersecurity threats. They can realize the risk of using internet and able to react to the circumstances effectively in their real life. However, there is limitation in the proposed system. This solution required a computer with ideal hardware specification, which may be costly, to run due to the game designed in an attractive graphic. Low-income household may not afford to own one. The research in the solution to raise the awareness of cybersecurity especially in schools is still less. It is recommended to have research focus on that in the future. Also, this game is still having the improvement spaces to get better in order to make the game more interesting and attracting to the Youngs. Thus, cybersecurity awareness will be increases in the future.

ACKKNOWLEDGMENTS

Highest appreciation to Asia Pacific University, Malaysia for the opportunity on the article publication.

REFERENCES

[1] Zainal Amin Ayub & Zuryati Mohamed Yusoff. Right of online information privacy of children in Malaysia: A statutory Perspective, 2018 (7) p.221-241

[2] Ahmad, N. and Othman, N. Information Privacy Awareness Among Young Generation In Malaysia. Journal of Science, Technology and Innovation Policy, 5(2) 2021, p.1-10 DOI: https://doi.org/10.11113/jostip.v5n2.41

[3] Rieff I (2018) Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach. Master thesis submitted in partial fulfilment of the requirements for the degree of Master of Science. Delft University of Technology.

[4] Hamed T. Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. 2016 Switzerland: Helvetic Editions LTD. DOI: http://dx.doi.org/10.2139/ssrn.3205035

[5] Beglar, D & Nemoto, T. Developing Likert-scale questionnaires. In N. Sonda & A. Krause, JALT2013 Conferences Proceedings. 2014 Tokyo: JALT.

[6] Gill, P., Stewart, K., Treasure, E. et al. Methods of data collection in qualitative research: interviews and focus groups. British: Dental Journal 204, 2008 291–295. DOI: https://doi.org/10.1038/bdj.2008.192

[7] DJ Borkovich, RJ Skovira. Working from Home: Cybersecurity in the Age of COVID-19. Issues in Information Systems, 21(4) 2020 pp.234-246

[8] Asokhia M.O. Enhancing National Development and Growth through Combating Cybercrime/Internet Fraud: A Comparative Approach. 23. 2010 p.13-19. DOI: https://doi.org/10.1080/09718923.2010.11892806

[9] Al-Sherbaz, A, Hendrix, M.,. and Bloom, V. Game Based Cyber Security Training: are Serious Games suitable for cyber security training? International Journal of Serious Games, 3 (1) 2016 p53-61. DOI: http://dx.doi.org/10.17083/ijsg.v3i1.107

[10] Sarker, I.H., Kayes, A.S.M., Badsha, S. et al. Cybersecurity data science: an overview from machine learning perspective. J Big Data 7, 41 2020. https://doi.org/10.1186/s40537-020-00318-5.

[11] N.-Z. Legaki, N. Xi, J. Hamari, K. Karpouzis, and V. Assimakopoulos. The effect of challenge-based gamification on learning: An experiment in the context of statistics education. International Journal of Human-Computer Studies, 144(12), 2020 1. DOI: https://doi.org/10.1016/j.ijhcs.2020.102496

[12] Sofia M.S, Andreas J & Matthias S. Capturing the complexity of gamification elements: a holistic approach for analyzing existing and deriving novel gamification designs. European Journal of Information Systems. 29(6), 2020 p.641-668. DOI: https://doi.org/10.1080/0960085X.2020.1796531

[13] Arwa A. Al Shamsi. Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE. Faculty of Engineering and IT, The British University in Dubai, UAE. 3(2), 2019 pp.8-29

[14] Zichermann, G., & Cunningham, C. Gamification by design: Implementing game mechanics in web and mobile apps. Gravenstein Highway North: O'Reilly Media, Inc. 2011

[15] Abawajy, J. User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 2014 pp.236-248. DOI: https://doi.org/10.1080/0144929X.2012.708787

[16] Zulkifli, Z., Abdul Molok, N. N., Abd Rahim, N. H., & Talib, S. Cyber Security Awareness Among Secondary School Students in Malaysia. Journal of Information Systems and Digital Technologies. 2(2), 2020 p.28-41.

[17] Zahri, Y., Susanty, A.H., & Mustaffa, A. Cyber Seity Situational Awareness among Students: A Case Study in Malaysia. 11, 2017 p.1704-1710. DOI: https://doi.org/10.1007/0-387-33406-8_37

[18] Papadakis, S, Marios Trampas, A, Barianos, A.K, Kalogiannakis, M, Vidakis, N. 'Evaluating the Learning Process: The "ThimelEdu" Educational Game Case Study', In Proceedings of the 12th International Conference on Computer Supported Education (CSEDU 2020), Prague, Czech Republic, 2, 2020 pp. 290–298

[19] Drace K. Gamification of the Laboratory Experience to Encourage Student Engagement. Journal of Microbiology and Biology Education. 14(2), 2013 p.273-274. DOI: http://dx.doi.org/10.1128/jmbe.v14i2.632

[20] Schöbel, S., Janson, A., Jahn, K., Kordyaka, B., Turetken, O., Djafarova, N., Saqr, M., Wu, D., Söllner, M., Adam, M., Gad, P. H., Wesseloh, H., & Leimeister, J. M. A Research Agenda for the Why, What, and How of Gamification Designs: Outcomes of an ECIS 2019 Panel. Communications of the Association for Information Systems, 46, 2020 pp.706-721. DOI: https://doi.org/10.17705/1CAIS.04630

[21] Cox, R., Firestone, D., Kubik, O., Olano, M., Oliva, L., Sherman, A., Patil, M., Seymour, J., Sohn, I., and Thomas, D. 2014 "SecurityEmpire: Development and Evaluation of a Digital Game to Promote Cybersecurity Education". USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14).

[22] Alias A, Aguilar-Parra JM, Camacho-Lazarraga P, Guerrero MA, Guerrero-Puerta L, Manzano-León A, Trigueros R,. Between Level Up and Game Over: A Systematic Literature Review of Gamification in Education. 2021 13(4). DOI: https://doi.org/10.3390/su13042247

[23] Hansen, L., & Nissenbaum, H.. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53(4), 2009 p.1155-1175.

[24] Zuriani Ahmad Zukarnain1*, Mimi Zazira Hashim, Norrini Muhammad, Farah Ahlami Mansor, W, & Nor Hazimah Wan Azib5. Impact Training on Cybersecurity Awareness. Gading Journal of Science and Technology, 3(1), 2020 p.114-120

[25] Khalid F, Rahman N.A.A, Sairi I. H, and Zizi N. A. M,. The importance of Cybersecurity Education in School. International Journal of Information and Education Technology, 10(5), 2020 p. 378-382

[26] D.S. Cruzes, L. Jaccheri, and F. Quayyum, Cybersecurity Awareness for Children: A Systematic Literature Review. International Journal of Child-Computer Interaction, 30 2021

[27] Adamu Abdullahi Garba, Fathe Jeribi, Ibrahim Al-Shourbaji, Mohammed Alhameed, Faheem Reegu, Sophia Alim. An Approach to Weigh Cybersecurity Awareness Questions In Academic Institutions Based On Principle Component Analysis: A Case Study Of Saudi Arabia. International Journal of Scientific & Technology Research, 10(4), 2021 pp.319-326

[28] J. Krath, L. Schurmann, Harald 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, 125, 2021.

[29] L. Tan, K. Yu, F. Ming, X. Cheng, G. Srivastava, “Secure and Resilient Artificial Intelligence of Things: a HoneyNet Approach for Threat Detection and Situational Awareness”, IEEE Consumer Electronics Magazine, 2021, doi: 10.1109/MCE.2021.3081874.

[30] L. Tan, N. Shi, K. Yu, M. Aloqaily, Y. Jararweh, “A Blockchain-Empowered Access Control Framework for Smart Devices in Green Internet of Things”, ACM Transactions on Internet Technology, vol. 21, no. 3, pp. 1-20, 2021,https://doi.org/10.1145/3433542.

[31] Z. Guo, K. Yu, A. Jolfaei, A. K. Bashir, A. O. Almagrabi, and N. Kumar, “A Fuzzy Detection System for Rumors through Explainable Adaptive Learning”, IEEE Transactions on Fuzzy Systems, doi: 10.1109/TFUZZ.2021.3052109.

[32] K. Yu, M. Arifuzzaman, Z. Wen, D. Zhang and T. Sato, “A Key Management Scheme for Secure Communications of Information Centric Advanced Metering Infrastructure in Smart Grid,” IEEE Transactions on Instrumentation and Measurement, vol. 64, no. 8, pp. 2072-2085, August 2015.

[33] Parameshachari, B.D. and Panduranga, H.T., 2021. Secure Transfer of Images Using Pixel-Level and Bit-Level Permutation Based on Knight Tour Path Scan Pattern and Henon Map. In Cognitive Informatics and Soft Computing (pp. 271-283). Springer, Singapore.

[34] Kowsalya, T., Babu, R.G., Parameshachari, B.D., Nayyar, A. and Mehmood, R.M., 2021. Low Area PRESENT Cryptography in FPGA Using TRNG-PRNG Key Generation. CMC-COMPUTERS MATERIALS & CONTINUA, 68(2), pp.1447-1465.

[35] Parameshachari, B.D., Kiran, R.P., Rashmi, P., Supriya, M.C., Rajashekarappa and Panduranga, H.T., 2019, January. Controlled partial image encryption based on LSIC and chaotic map. In ICCSP (pp. 60-63).

[36] Nguyen, T., Liu, B.H., Nguyen, N., Dumba, B. and Chou, J.T., 2021. Smart Grid Vulnerability and Defense Analysis Under Cascading Failure Attacks. IEEE Transactions on Power Delivery.

[37] Nguyen, T.N., Liu, B.H., Nguyen, N.P. and Chou, J.T., 2020, June. Cyber security of smart grid: attacks and defenses. In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[38] Shahriar, Md Rakib, SM Nahian Al Sunny, Xiaoqing Liu, Ming C. Leu, Liwen Hu, and Ngoc-Tu Nguyen. "MTComm based virtualization and integration of physical machine operations with digital-twins in cyber-physical manufacturing cloud." In 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 46-51. IEEE, 2018.

[39] Nagaraj, V., Sumithira, T.R. and Prabu, S., 2016. Development of Communication Technologies and Networks for Smart Grid. International Journal of MC Square Scientific Research, 8(1), pp.81-92.

[40] Arun, M., Baraneetharan, E., Kanchana, A. and Prabu, S., 2020. Detection and monitoring of the asymptotic COVID-19 patients using IoT devices and sensors. International Journal of Pervasive Computing and Communications.