

Cybersecurity Awareness Among Teenagers and Children Using Self-Learning System

Summetha Parimalam¹, Intan Farahama Binti Kamsin², Zety Marlia Zainal Abidin³, Hemalata Vasudavan⁴,
^{1,2,3,4}Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur,
Malaysia.
¹summethaparimalam23@gmail.com, ²intan.farahana@staffemail.apu.edu.my, ³zety@staffemail.apu.edu.my,
⁴hemalata@staffemail.apu.edu.my

Abstract— This study is to research on solutions to create awareness among teenagers and children through independent learning. The cybersecurity threats faced by teenagers and children has been increasing. Research have been conducted to study the current cyber security issues that children and teenager face as well as current solutions available to educate them on cybersecurity issues. The pros and cons of current available system and ideas to innovate the current system to provide better exposure on cybersecurity awareness have been studied. Probability sampling technique with stratified sampling technique have been suggested to study the data obtained through survey forms. The results from this research will be used to design a self-learning cybersecurity education system for children and teenagers. This will ensure that healthy internet behaviors among children and teenagers from the Gen Z will be aided.

Index Terms - Awareness, Curriculum, Cyber Attacks, Cyber Threat, Education, Game, Self-learning, System

1.0 Introduction

In today's generation, almost everyone is involved with technology. However, the fact that it also holds a large amount of risk should not be ignored [1]. Many terms such as security online, as well as internet security and cybersecurity are widely used today because on the evolution of technology and the risk these technologies carry [1].

Ever since the COVID-19 pandemic, children and teenagers have been spending quite number of hours per day on their technologies as well as on the internet. Since teenagers and children are spending more time with their devices, their curiosity will lead them to explore more over the internet [1]. Teenagers and children are not well equipped with knowledge to be able to assess the good and bad of the internet [2]. Furthermore, teenagers and children can be scammed into sending details of themselves if they are not careful enough [3]. Many teenagers who are below 20 have been found involved in scams where they have lost a significant amount of money [3]. The diagram below

shows the rise in the percentage of age groups being scammed online.

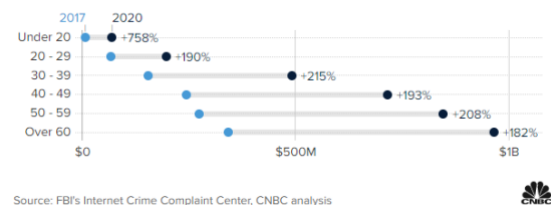


Figure 1: FBI's Internet Crime Complaint [3]

Based on figure 1, individuals under the age of 20 has the highest raise in percentage from the year of 2017 to the year of 2020 for being involved in online scams [3].

Therefore, this research is to find a solution to educate teenagers and children regarding the cyber field. In this study, cyber knowledge is being defined as the information needed to be gained by individuals to protect themselves from cyber-attacks and threats.

2.0 Literature Review

The development of technology today has also increased the number of issues caused by it. Based on research done by Ng Jia Jian and Inten Farhana Binti Kamsin, (2021) they have stated the Malaysian Communication and Multimedia Commission (MCMC) mentioned that there is an average of 6.6 hours spent by people online daily on the year of 2018 [4]. Furthermore, Malaysia is known to be the second in Asia for youth bullying [5]. A research paper based on a case study of Saudi Arabia has stated that younger individuals hold a greater risk in being the victim to the cyber world [6]. This is because they are more curious and adventurous towards everything, they discover newly without knowing the good and bad of it [6]. Furthermore, the youths who are from the age of 13 years old to the age of 15 years old have the highest frequency in being the easy target towards cyber threats and attacks as they have poor background in cybersecurity [7].

There have been solutions introduced to raise cybersecurity awareness among teenagers and children as

they have been the easy target to cyberbully, cyber threats as well as cyber-attacks. One of the solutions that have been introduced is to use video-based method to deliver the idea on security awareness in using technology. Tonia San Nicolas-Rocca, Benjamin Schooley and Janine L. Spears, (2014) have conducted a study and came up to conclusion that video based method are effective in raising the awareness on cybersecurity. Another method is to create awareness through games based on the field. An interview has been conducted by Arwa A.Al Shamsi to study the awareness level of the children as well as the preferred ideas on how awareness should be given [8]. The table below shows the output of the interview.

Interview Question	Interview No. 1	Interview No. 2	Interview No. 3
1.1 What online risks children may expose to?	-Cyber Bullying -Identity Theft -Online Phishing -Pornography	-cyber bullying -pornography -break to privacy -sharing personal information.	-online bullying -viruses that may destroy the computers -break to the privacy of children -identity theft
1.2 What are the topics of the security awareness that children learn about?	-Cyber Bullying -Privacy -Password -Online safety -Online protection -phishing -Identity theft -online strangers	-identity theft -cyber bullying -online protection -phishing -securing private information -password security	-identity theft -password protection -Internet safety best practices -cyber bullying -privacy
2.1 Can you give an example to show how the awareness program influenced children's online behavior?	- more secure while playing online games - aware of phishing - transfer their knowledge to their family members	-students became more cautious when using the Internet -students become more caring about their personal information -Students become more aware while playing online games to some issues such as pornography	-students become more aware -students create strong passwords and they don't use the same password for all of their accounts -students stop giving their private information online
3.1 Do you think that this awareness program is effective? To what extent?	Yes, very effective in raising the cyber security awareness level among students	-Too effective to raise sufficient awareness among students and to sensitize them not to share their personal information -Students learned to protect themselves and be more aware while using the Internet.	Yes, cyber security awareness is very effective in raising the awareness level and affecting student's behavior online
3.2 What are the limitations in the cyber security awareness program?	Too narrative, more awareness videos should be added as well as training offered through video games	narrative more videos should be added -the curriculum should include more video games and hands-on activities about the topics.	-more narrative, tends to be somewhat static -more short films and video clips should be added to the Cyber Security Awareness program

Figure 2: Output of interviews conducted by Arwa AAl Shamsi (Part 1)[8]

3.3 What are your suggestions to increase the effectiveness of the cyber security awareness program?	Society engagement in awareness to build security culture among society.	-awareness training for parents to recognize online risks and then engage in educating their children and protect them. -all society should be aware of internet best practices in order to achieve a more secure society. -Media should participate in the awareness program and telecommunication companies as well.	-parent's engagement in cyber security awareness training -society should be engaged in the cyber security awareness programs especially the media. -Awareness posters should be set in public places -awareness messages should be sent to citizens to build strong security culture among society
Main Themes that have emerged out of the interview	-Cyber Bullying -Identity Theft -Online Phishing -Pornography -phishing -password -privacy -Effective -narrative training -social engagement	-cyber bullying -pornography -break to privacy -privacy -password -effective -narrative training -phishing -Identity theft -parents awareness -media engagement	-identity theft -password protection -Internet safety best practices -cyber bullying -privacy -phishing -viruses -effective -narrative training -parents' engagements Awareness posters and messages

Figure 3: Output of interviews conducted by Arwa A.Al Shamsi (Part 2)[8]

Based on the interview conducted towards school students, the respondents mostly prefer videos on awareness as well as online games related to the field and hands on practices related to the topics that have been studied [8]. Based on the research that was conducted towards school students, teachers, and parents in Klang Valley, 50% of the teachers find that it is important to regulate cybersecurity education in the school's syllabus [9]. However, there has not been a clear module or platform endorsed by the government for the formal education [9].

Aside from conducting lectures, and showing videos, another concept introduced was also gamification which was earlier found in the paper by Al Shamsi. Gamification can be said to be the application of gaming in a field of study to motivate people to be educated on that field [10]. However, this method only involves games and not notes and resources on the concepts that are learned through the game [10]. Several concepts that have been introduced in this method includes, puzzles, quest, mission, adventure types of games [11]. These games include basic knowledge of cybersecurity however they are not being explained in depth [10].

Based on the above collection of research, to create awareness among teenagers and children on cybersecurity, gamification or lectures conducted by teachers are mostly suggested. However, the only self-learning method is gamification where they learn concepts through games but not in depth as in lectures conducted by teachers. Therefore, based on the research, a system with not only a curriculum with videos, resources, games but also other options such as news portal, contact services should work the best to educate the teenagers and children on cybersecurity. This is supported by Cybersecurity Malaysia (CSM) that uses similar approaches which is having an online portal that includes, tips, games, quizzes, videos, and newsletters [12].

3.0 Research Domain

3.1 Cybersecurity Awareness Among Teenagers and Children

The availability of internet and technology have increased the usage of both by children and teenagers around the world [1]. Today, there has been many unknown risks that the internet possesses [9]. A survey report by the DiGi CyberSAFE have stated that teenagers and children have been facing several types of cyber risk [9]. This is due to the lack of knowledge on cyber safety and cybersecurity that these group of individuals possess [9]. These individuals do not know how to differentiate between opportunities and risk on the internet [1]. Hence, this led them to exploring

everything without being cautious [1]. In conclusion, teenagers and children of generation Z are individuals who uses the internet and technology in a high rate, and they are lack in knowledge on protecting themselves from cyber risk that the internet and technology possess [9]. Therefore, to overcome this issue, these individuals must be educated and updated with current trends on cyber security risk since technology is known to be developing from time to time. Solutions to this issue must be identified to prevent these individuals from being exploited and exposed to cyber risks.

3.2 Current Cybersecurity Awareness Solutions

The current solutions that have been existing is course curriculum conducted by teachers, games online and surfing through the net to obtain latest news on cyber risks [8]. As for the course curriculum, it needs to be assisted by a teacher as only the teachers have the course outline and materials [8]. As for the games, the games only help teenagers and children learn the basic terms and application and not in depth [11]. The games are based on basic knowledge which can be gained from the ICT subject the school has itself [11]. It does not consist of information on updated trends [8]. As for the news on cyber risks, there are too many resources on the internet, however the teenagers and children need to have the interest to read the news on their own [8]. All the current solutions available, needs to be assisted, or they have only basic information or needs the teenagers and children to gather information on their own through the internet [8]. In conclusion, these each of the solutions that exist, have their own cons and gaps. However, they still provide awareness but not in the most efficient and effective way [8]. Therefore, by combining the pros of each solution, the gaps can be removed, and a proper solution can be obtained.

3.3 Self-learning on Cybersecurity Awareness

Most solutions provided such as campaign and the education system introduced by schools needs assistance of people [2]. However, the self-learning solutions are either online site that provides basic information on cybersecurity, games related to cyber security and online news platform to be updated on current cyber trends [2]. These self-learning solutions are all available separately which is inconvenient to the teenagers and children as they need to use various platforms to educate themselves. Teenagers and children get easily distracted when they have several tasks to perform on separate platforms [2]. Therefore, they might be excited to begin at first, however, eventually they will lose their consistency and give up [2]. In conclusion, the self-learning platforms and solutions that are available now is not very efficient to teenagers and children as it requires so much effort in accessing the materials to educate themselves [2]. Therefore, to overcome this gap, a system that consists of all materials such as, the curriculum based on cybersecurity chapters, games, news portal and authority contact should be created [2]. This system will be convenient to be used by teenagers and children as all these options are available under one platform as well as they will be motivated to educate themselves using this system.

4.0 Similar System

There were several similar systems identified. However, from the collection of similar system, two of the systems characteristics are being studied.

System Name	eSafety Commissioner	Interland
Type of system (Application/Website)	Website	Website
Targeted user	Educators, parents, young people, kids, women, senior citizen, diverse group, industries	Primary school students
Types of Resources	- Information on cyber related topics for parents, young people, kids, women, senior citizen, diverse group, industries - Classroom resources for Educators	No resources
Requires adult's assistance	Yes (for educators)	No
Games	No	Yes
News Portal	Yes	No
Cybersecurity Tips	Yes	No
Region of Usage	Australia	World-wide

Table 1: Comparison between two similar systems

Table 1 shows the comparison between two similar systems which are eSafety Commissioner which is owned by the Australia government for the Australians and Interland which can be used worldwide by anyone.

4.1 eSafety Commissioner

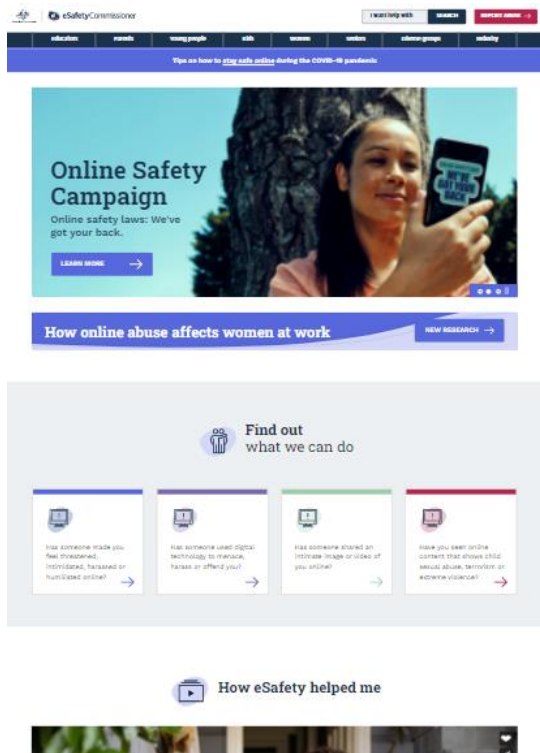


Figure 4: Main Page [13]

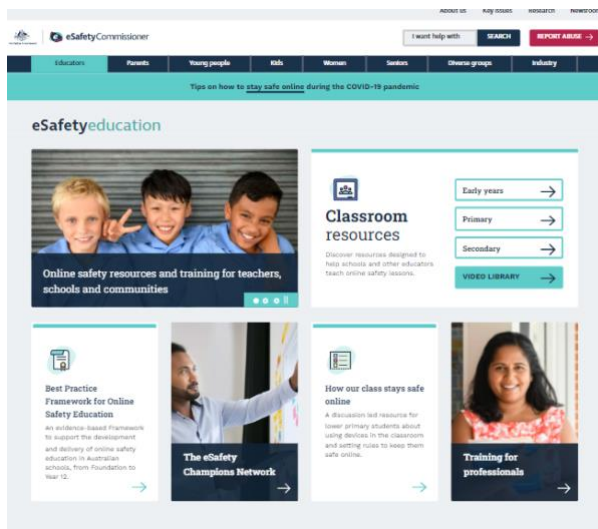


Figure 5: Educator Page [13]

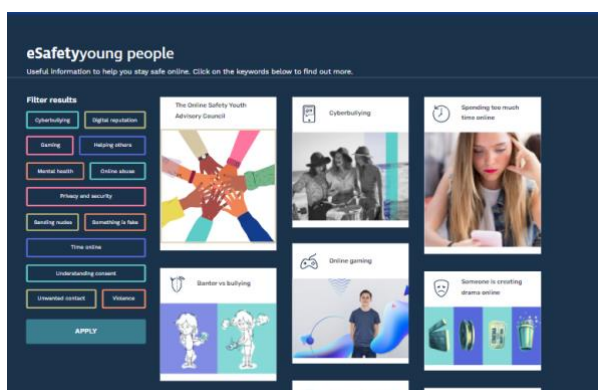


Figure 6: Young People Page [13]



Figure 7: Kids Page [13]

Figure 5 until 7 shows several pages that can be found in eSafety commissioner. This website focuses on several users. However, based on this research, the main functions that being compared to is the educator, young people, and kids. This website only focuses on resources and information. There are no online games that can be found. Furthermore, this system requires adult assistance to access through the educator resources.

4.2 Interland



Figure 8: Interland Main Page [14]

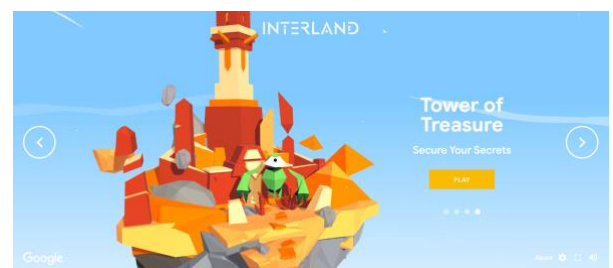


Figure 9: First Quest in Interland [14]

Figure 8 and 9 shows the Interland pages. Interland is a game-based learning platform that only provides quest to be solved and there are no resources, cyber tips or news provided.

5.0 Problem Statement

The development of technology and the existence of the internet today have benefited many people as well as raised some concerns [15]. Globally, organizations are seen as the focus in every cyberthreats. Many prevention methods and solutions to cyber problems are taken to protect companies. However, there are very few research on cyber safety of children and teenagers who are mostly exposed to the internet with minimal knowledge to protect themselves from cyber threats as well as cyberbullying [16]. On 14th January 2022, The Star newspaper have published a news stating that Malaysia is in the second place in Asia for cyberbullying [5]. Furthermore, during the COVID-19 pandemic in the year of 2020, many teenagers have been scammed and blackmailed into sending their explicit photos through Facebook [17]. This led their explicit photos to be distributed around without their consent in a telegram group known as V2K [17]. Based on several research, it has been known that games and resources related to cybercrimes, cyber safety and cyberthreats have been created to educate teenagers. Therefore, another solution with the aid of cybersecurity tools and knowledge on enhancing this idea is needed to be investigated to create a better exposure for teenagers towards this era where the technology is constantly evolving, and threats are developing in many forms.

6.0 Research Aims

This study aims to develop an efficacious system to educate teenagers and children to have better exposure on cyber related knowledge by centralizing the below objectives:

7.0 Research Objectives

- i. To implement resources and notes on cyber related topic in the system
- ii. To develop games and quiz in the system
- iii. To create a news portal on recent cyber-attacks and threats
- iv. To develop option to contact authorities

8.0 Research Significance

This study will ensure that a solution is provided into helping teenagers and children to obtain awareness on cybersecurity issues on their own. This group of people will obtain a better understanding on awareness they need to ensure they are not being exploited by the cybersecurity threats. This prevents them from being the victim of cyber threats such as scam, bullying, phishing and many more. The solution to overcome this problem is to create a system, an

enhanced version of existing systems by comparing the previous systems and programs that have been developed to create cybersecurity awareness among teenagers.

In addition to that, this research will specifically assist to identify the weaknesses of current available systems and solutions to overcome it as well as how to develop the system to accommodate the solutions.

9.0 Research Methodology

The target users for the system in this research are teenagers and children. This system has the purpose to create awareness among teenagers and children on cybersecurity awareness. This research will be using probability sampling technique where a survey form is distributed to a sample of the population selected which is the primary school and secondary school students. In probability sampling, a stratified random sampling is used where school students from a government school are selected. And they are further split into two strata which are primary and secondary. To obtain the data, surveys are used as data collection method. This survey consists of both open and close ended questions. And this survey will be created using Google forms.

10.0 Overview of the Proposed System

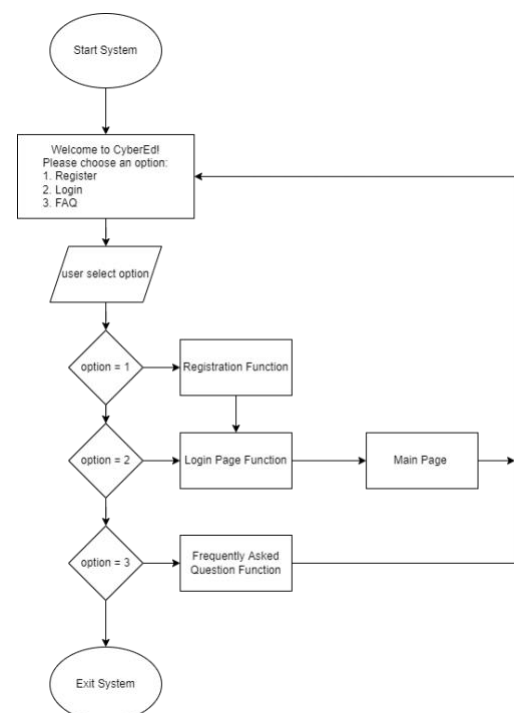


Figure 10: Proposed System Page

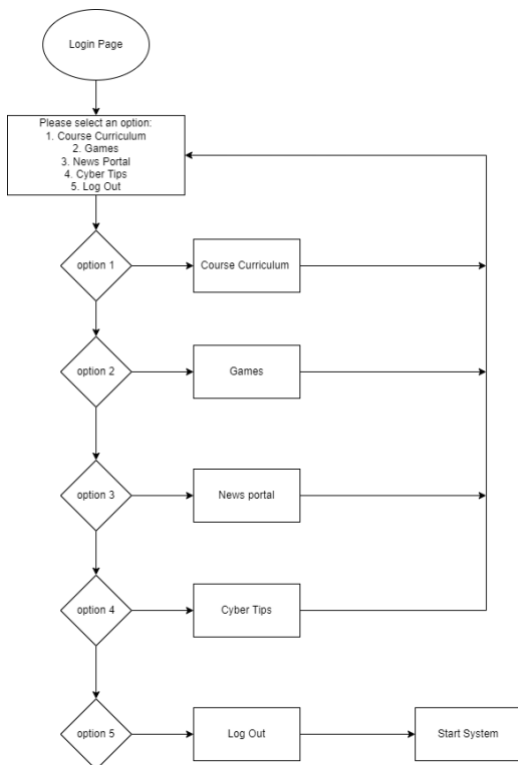


Figure 11: Main Page

Figure 10 shows the proposed system overview page while figure 11 shows the main page flow of the suggested functions to be included. From figure 10, the proposed system allows user to choose from 3 options which is to register, login and view the frequently asked questions. Registration function will request the user to register themselves with details such as name, age, school name, school type, parents name, parents contact number and many more. Figure 11 shows the main page which consist of 5 functions which are, course curriculum, games, cyber security tips and logging out of the system.

11.0 Conclusion

Today, cybersecurity awareness is important and necessary among teenagers and children. This is because, they have been using technology and internet mor frequently without being aware of the bad that technology and the internet brings [18]. Their lack of information on the internet and technology will lead them to be involved in cybersecurity threats such as scamming, phishing, and cyber bullied. This research will ensure that teenagers and children have better exposure to cybersecurity education in an easy way without the need of adult's assistance throughout the cybersecurity awareness gaining process. If solution to overcome the issue where children and teenager are exposed to cybersecurity issues are not created, these group of people are more vulnerable to the internet and technology which leads to increase in crime rate in the country as well. More research and innovation are encouraged to overcome this issue to prevent teenagers and children from being the victim of cybersecurity issue.

References

- [1] Quayyum, F., Cruzes, D. and Jaccheri, L., 2021. Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30(2), pp.1-26. <https://doi.org/10.1016/j.ijcci.2021.100343>
- [2] Zilka, G., 2017. Awareness of eSafety and Potential Online Dangers among Children and Teenagers. *Journal of Information Technology Education:Research*, 16(1), pp.319-338. <https://doi.org/10.28945/3864>
- [3] O'Brien, S., 2021. *Tech-savvy teens falling prey to online scams faster than their grandparents*. [online] CNBC. Available at: <https://www.cnn.com/2021/08/10/tech-savvy-teens-falling-prey-to-online-scams-faster-than-their-grandparents.html>
- [4] Ng, J. and Kamsin, I., 2021. Cybersecurity Awareness Among the Youngs in Malaysia by Gamification. *Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)*, 4(1), pp.487-494. <https://doi.org/10.2991/ahis.k.210913.061>
- [5] The Star. 2022. *Malaysia is 2nd in Asia for youth cyberbullying*. [online] Available at: <https://www.thestar.com.my/news/nation/2022/01/14/malaysia-is-2nd-in-asia-for-youth-cyberbullying>
- [6] Garba, A., Jeribi, F., Al-Shourbaji, I., Alhameed, M., Reegu, F. and Alim, S., 2021. 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), pp.319-326.
- [7] Ahmad, N. 'Ain ., & Othman, N. . (2021). Information Privacy Awareness Among Young Generation in Malaysia. *Journal of Science, Technology and Innovation Policy*, 5(2), 1–10. <https://doi.org/10.11113/jostip.v5n2.41>
- [8] Al Shamsi, A., 2019. Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE. *International Journal of Information Technology and Language Studies (IJITLS)*, 3(2), pp.8-29. <https://doi.org/10.13140/RG.2.2.28488.14083>
- [9] Zulkifli, Z., Abdul Molok, N. N., Abd Rahim, N. H., & Talib, S. (2020). Cyber Security Awareness Among Secondary School Students in Malaysia. *Journal of Information Systems and Digital Technologies*, 2(2), 28–41. Retrieved from <https://journals.iium.edu.my/kict/index.php/jisdt/article/view/151>
- [10] San Nicolas-Rocca, T., Schooley, B. and Spears, J., 2014. Exploring the Effect of Knowledge Transfer Practices on User Compliance to IS Security Practices. *International Journal of Knowledge Management*, 10(2), pp.62-78. <https://doi.org/10.4018/ijkm.2014040105>
- [11] Rieff, I. (2018). Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach.
- [12] Abd Rahim, N., Hamid, S., & Mat Kiah, M. (2019). ENHANCEMENT OF CYBERSECURITY AWARENESS PROGRAM ON PERSONAL DATA PROTECTION AMONG

YOUNGSTERS IN MALAYSIA: AN ASSESSMENT. *Malaysian Journal Of Computer Science*, 32(3), 221-245. <https://doi.org/10.22452/mjcs.vol32no3.4>

- [13] *Office of the eSafety Commissioner*. Healthdirect.gov.au. (2022). Retrieved 16 May 2022, from [https://www.healthdirect.gov.au/partners/office-of-the-esafety-commissioner#:~:text=The%20eSafety%20Commissioner%20\(eSafety\)%20is,our%20resources%20and%20Outreach%20Program.](https://www.healthdirect.gov.au/partners/office-of-the-esafety-commissioner#:~:text=The%20eSafety%20Commissioner%20(eSafety)%20is,our%20resources%20and%20Outreach%20Program.)
- [14] *Play Interland - Be Internet Awesome*. Play Interland - Be Internet Awesome. (2022). Retrieved 16 May 2022, from https://beinternetawesome.withgoogle.com/en_us/interland.
- [15] Agbeko, M. (2021). Understanding Cyber Safety Behavior Among Teenagers in Ghana. *International Journal Of Computer Science And Information Security (IJCSIS)*, 19(6). <https://doi.org/10.5281/zenodo.5111963>
- [16] Schöbel, S., Janson, A. and Söllner, M., 2020. Capturing the complexity of gamification elements: a holistic approach for analysing existing and deriving novel gamification designs. *European Journal of Information Systems*, 29(6), pp.641-668
- [17] Hakim, A., 2020. *Victims Of V2K Telegram Group Come Forward To Report Abuse | TRP*. [online] TRP. Available at: <https://www.therakyatpost.com/news/malaysia/2020/10/06/victims-of-v2k-telegram-group-comes-forward-to-report-abuse>
- [18] Yan, Z. (2009). Limited Knowledge and Limited Resources: Children's and Adolescents' Understanding of the Internet. *Journal Of Applied Developmental Psychology*, 30(2), 103-115. <https://doi.org/10.1016/j.appdev.2008.10.012>

