INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 14, Issue 8, (2024) E-ISSN: 2222-6990

Exploring Cyber Security Behavioral Practices among Secondary School Students Following the Mydigital Maker Champion Program in Putrajaya, Malaysia

Intan Diana[1,2], Ismi Arif Ismail[1,2], Mohd Zairul[1,3]

[1]Institute Social Science Studies, Universiti Putra Malaysia, Serdang, 43400, Selangor, Malaysia, [2]Faculty of Educational Studies, Universiti Putra Malaysia, [3]Department of Architecture, Faculty of Design and Architecture, Universiti Putra Malaysia

Email: intanabrahman@gmail.com

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v14-i8/22553 DOI:10.6007/IJARBSS/v14-i8/22553

Published Date: 15 August 2024

Abstract

The practice of cyber security behaviour is the act of protecting digital devices and oneself from cyber threats. Cases of cyber threats increasing year by year have negatively affected the victims, such as loss of money, properties and emotional disturbance. Furthermore, teenagers are the most internet users at risk of being exposed to cyber threats. By using the Technology Threat Avoidance Theory, the Knowledge, Attitude, and Practice Model, and the Theory of Planned Behaviour, this study explores the problem of cyber threats that occurs to high school students who follow the MyDigital Maker Champion program in Putrajaya, Malaysia, understanding the students' cybersecurity behaviour practices as well as exploring methods of overcoming the problem of cyber threats among students. Next, this study proposes a cybersecurity behavioural framework with components to solve cyber threats among the students. This study uses an interpretive paradigm with a case study design. Qualitative data was obtained through interviews, focus groups, and archival document analysis of cyber security experts, teachers, school counsellors, and high school students who followed the MyDigital Maker Champion program. Data were analysed by conducting a thematic analysis. The study's findings show that there are four types of cyber threats, from the point of view of 1) the Information Technology Policy Act, 2) media content, 3) writing, and 4) psychology. In addition, there are two forms of cyber security behaviour practices, which are 1) strict cyber security practices and 2) being ethical in surfing cyberspace. This study also found three methods to overcome the problem of cyber threats, namely 1) awareness campaigns, 2) receiving support from subjective norms, and 3) implementing cyber security laws specifically for the teenagers. The findings of this study also form a framework of cyber security behaviour that help to overcome the problem of cyber threats that occurs

among high school students. In conclusion, the findings of this study can guide students, teachers, and the Malaysian Ministry of Education to improve the solution method in facing cyber threats among high school students through education and produce a future learning system that is more advanced, quality and guaranteed security from any form of cyber-attack.
Keywords: Cybersecurity, Behavioural Practices, High School Student, Mydigital Maker Champion, Putrajaya

Introduction

Malaysia has grown by 155 per cent of internet users since 2016, when there was a rise of 18.4 per cent, and by 47 per cent in 2020 (MCMC, 2020). Teenagers represent most internet users, accounting for more than 70% of all users globally (ITU, 2021). According to Statistica (2019), it is utilised by 73.4 per cent of secondary school students. Malaysia had a 974-case, or 11 per cent, rise in cyber threats between 2020 and 2021. This statistic means that cyber threats are becoming severe and worrying. The growing use of the internet increases an individual's vulnerability to cyber-attacks. In contrast to other states in Malaysia, Putrajaya has the highest percentage of internet users (DOS, 2021). Hence, the study has four specific objectives: (1) Explore the problem of cyber threats for high school students who follow the MyDigital Maker Champion program in Putrajaya, Malaysia. (2) Understanding the cyber security behaviour practices of high school students who follow the MyDigital Maker Champion program in Malaysia. (3) Exploring methods to overcome the problem of cyber threats among high school students who follow the MyDigital Maker Champion program in Putrajaya, Malaysia and (4) Forming a cyber security behaviour framework that has components of steps to solve the problem of cyber threats occurring among secondary schools' students that follow the MyDigital Maker Champion program in Putrajaya, Malaysia.

Since most secondary school students already own smartphones (Zahri et al., 2017), they are more likely to utilise the Internet (Zulkifli et al., 2020). If people don't know how to employ cyber security in their daily lives, they are more likely to be subjected to assaults (Rahman et al., 2020). It is crucial to practice cyber security behaviour, in the purpose of protecting computers and smartphones from cyber threats like viruses, malware, ransomware, worms, trojans, adware, phishing (Egelman et al., 2016), fraud and theft through cyberspace (Pitchan & Omar, 2019). Firstly, device security (device security) - (that is, using passwords on devices, installing antivirus software, and blocking fire) is one of the four basic categories of cyber security behaviour practice requirements, according to Egelman and Peer (2015). The second need is password creation, which refers to always utilising a password. The third requirement is proactive awareness, which refers to being aware of cyber-attacks or knowing how to defend against them. The fourth and last requirement is upgrading (updating), which refers to constantly updating antivirus software and passwords.

Therefore, to control the occurrence of cyber threats to secondary school students, several methods of overcoming cyber threats need to be done, such as providing a cyber security module (Rahim, 2019), the role of parents (Pitchan, 2017), the existence of cyber security laws need to be disseminated to the general public (Pitchan, 2017) and the importance of cyber security education knowledge in schools needs to be applied as early as possible (Aguayo, 2020; Aguayo et al., 2019; Li & Kulkarni, 2016; Malecki, 2018; Pencheva et al., 2020; Rahman et al., 2020). In addition, school-organized programs (Rahman et al., 2020; Zulkifli et al., 2020) emphasize that education through module learning (Zahri et al., 2017), gamification (Aguayo

et al., 2019; Jian & Kamsin, 2021; Li & Kulkarni, 2016) and competition (Bashir et al., 2017) are methods of overcoming cyber threats that are reported to be effective.

Methods

The interpretive paradigm is used as the research paradigm in this study since it relates to qualitative analysis (Merriam & Tisdell, 2016). The researcher used the qualitative research methodology because it is consistent with the primary goal of this study, which is, to investigate the cyber security behavioural practices involving the cyber world that occur among high school students in Malaysia who participate in the MyDigital Maker Champion programme, forming a final framework of students' cyber security behavioural practices. The case study method is used in this investigation. This study uses the case study approach because it refers to a unique explanation of a design, experience, and information that can be gathered from the interview with distinct informants.

Results and Discussion

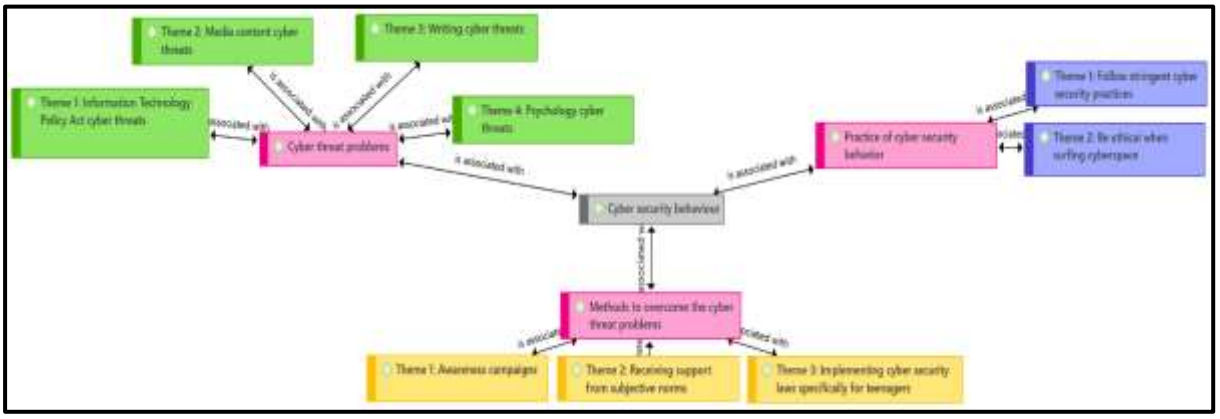

Figure 1: The final framework of the study (Researcher, 2023)

Figure 1 depicts the study's final framework, which includes the research findings. According to the study's conclusions, there are four sorts of cyber threats: 1) the Information Technology Policy Act cyber threats, 2) media content cyber threats, 3) writing cyber threats, and 4) psychology cyber threats. Most informants agree that hacking is the most widespread cyber risk issue among high school students. On the other hand, the love scam was the cyber threat most frequently mentioned by informants and discovered in most archive document research. According to the sources, foul language has become a common internet hazard in the lives of teenagers and high school pupils. Aside from that, cyberbullying is the most common hazard faced by high school students.

Furthermore, there are two types of cyber security behaviour practices: 1) follow stringent cyber security practices, and 2) be ethical when surfing cyberspace. Informants frequently communicate cyber threats through offensive content, vocal hate speech, and online games with criminal aspects. Privacy setting is the most effective and often discussed security screening technique, according to the informants. Other than that, most informants think that the most critical cyber security behavioural habit for high school children or teenagers to establish is visiting trustworthy websites.

This study also discovered three ways to deal with the issue of cyber threats: 1) awareness campaigns, 2) getting support from subjective norms, and 3) implementing cyber security laws specifically for teenagers. The informants most typically suggest growing cyber security

knowledge and following cyber security programmes. Adopting cyber security protection technology is another technique in tackling the problem of cyber dangers among high school students. Other than that, most interview agreed that a teen's ability to obtain family assistance is essential for overcoming the cyber threats. Finally, enacting rules specifically for teenagers is one strategy in tackling the problem of cyber hazards that affect high school students.

The results of this study also help to create a framework for cyber security behaviour practices that aid in addressing the cyber dangers which affect high school students who participate in Malaysia's MyDigital Maker Champion programme. As shown in Figure 1, this framework combines the themes drawn from the study questions and incorporates them with models and theories.

Conclusions

In a nutshell, the Malaysian Ministry of Education (MoE) may enhance the cyber security curriculum. Cybersecurity Malaysia can suggest special teen rules, the Multimedia Communications and Malaysia Commission (MCMC) can give new researchers access to reference material, and the Malaysian Digital Economy Corporation (MDEC) can improve students' learning materials. This study also contributes new knowledge by incorporating educational technology to the Technology Threats Avoidance Theory, Theory of Planned Behaviour, and Knowledge, Attitude, and Practice Model. In addition, the study's findings can help students, teachers, and the Malaysian Ministry of Education to improve the way they deal with cyber threats among high school students through instruction, leading to the creation of a future learning system that is more sophisticated of higher quality, and assured to be secure from all types of cyber-attacks.

References

Aguayo, G. A. C. (2020). *A visualization tool for cybersecurity education for high school students* (Issue December) [Doctoral dissertation, Purdue University]. https://doi.org/https://doi.org/10.25394/pgs.13379900.v1

Aguayo, G. C., Morales, U., Long, X., Niyaz, Q., Yang, X., & Javaid, A. Y. (2019). An introductory visualization aid for cybersecurity education. *15th International Conference on Frontiers in Education: Computer Science and Computer Engineering,(FECS 19)*, 10–15.

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security*, *65*, 153–165. https://doi.org/10.1016/j.cose.2016.10.007

DOS, D. of S. (2021). *Pocket Stats Q1 2021* (Issue May). https://doi.org/ISSN 26829053

Egelman, S., Harbach, M., & Peer, E. (2016). Behavior ever follows intention?: A validation of the Security Behavior Intentions Scale (SeBIS). *Conference on Human Factors in Computing Systems - Proceedings*, 5257–5261. https://doi.org/10.1145/2858036.2858265

Egelman, S., & Peer, E. (2015). Scaling the security wall : Developing a security behavior intentions scale (SeBIS). *Conference on Human Factors in Computing Systems - Proceedings*, *2015-April*, 2873–2882. https://doi.org/10.1145/2702123.2702249

ITU. (2021). Measuring digital development: Facts and figures. In *ITU Publications*. https://www.itu.int/en/mediacentre/Documents/MediaRelations/ITU Facts and Figures 2019 - Embargoed 5 November 1200 CET.pdf

Jian, N. J., & Kamsin, I. F. B. (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*, 487–494. https://doi.org/10.2991/ahis.k.210913.061

Li, C., & Kulkarni, R. (2016). Survey of cybersecurity education through gamification. *ASEE Annual Conference and Exposition, Conference Proceedings*. https://doi.org/10.18260/p.25981

Malecki, A. (2018). Cybersecurity in the classroom: Bridging the gap between computer access and online safety. In *Cyber Security Capstone Research Project Reports*. https://scholar.valpo.edu/cgi/viewcontent.cgi?article=1001&context=cscrpr

MCMC. (2020). Internet users survey 2020. In *Malaysian Communications And Multimedia Commission*. https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Internet-Users-Survey-2018-(Infographic).pdf

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative Research A Guide to Design and Implementation* (Fourth, Vol. 148). Jossey-Bass.

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security and Privacy*. https://doi.org/10.1109/MSEC.2020.2969409

Pitchan, M. A. (2017). Kesedaran dan amalan keselamatan siber dalam kalangan pengguna internet di Malaysia [Doctoral dissertation, Universiti Putra Malaysia]. In *UPM*. https://doi.org/10.17576/JKMJC-2019-3501-08

Pitchan, M. A., & Omar, S. Z. (2019). Dasar keselamatan siber Malaysia: Tinjauan terhadap kesedaran netizen dan undang-undang. *Jurnal Komunikasi: Malaysian Journal of Communication*, *35*(1), 103–119. https://doi.org/https://doi.org/10.17576/JKMJC-2019-3501-08

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Statistica. (2019). *Statistica*. Statistica. https://www.statista.com/statistics/973925/malaysia-smartphone-ownership-by-education/

Zahri, Y., Susanty, A. H. R., & Mustaffa, A. (2017). Cyber security situational awareness among students: A case study in Malaysia. *International Journal of Educational and Pedagogical Sciences*, *11*(7), 1704–1710. https://doi.org/https://doi.org/10.5281/zenodo.1131053

Zulkifli, Z., Molok, N. N. A., Rahim, N. H. A., & Talib, S. (2020). Cyber security awareness among secondary school students in Malaysia. *Journal of Information Systems and Digital Technologies*, *2*(2), 28–41. https://doi.org/doi.org/10.5281/zenodo.1131053