IMPACT OF TRAINING ON CYBERSECURITY AWARENESS

Zuriani Ahmad Zukarnain[1*], Mimi Zazira Hashim[2], Norrini Muhammad[3], Farah Ahlami Mansor[4], Wan Nor Hazimah Wan Azib[5]

[1]Faculty of Computer & Mathematical Sciences,
Universiti Teknologi MARA Kelantan, Bukit Ilmu, Machang, Kelantan, Malaysia

[2,3,4,5] Faculty of Business and Management,
Universiti Teknologi MARA Kelantan, Bukit Ilmu, Machang, Kelantan Malaysia

[*]Corresponding author: zurianiaz@uitm.edu.my

Abstract

Studies show that training is a good alternative to deliver cybersecurity knowledge to children. This paper reports on the findings of a study after conducting awareness training programs. The ultimate goal of the program is to help children to understand issues related to cybersecurity and instill the cybersecurity awareness. Children are now discovering computers, smartphones or tablets at an early age. Even though an internet connection of the computers and mobiles devices can be useful for learning as well as enhancing social relations and keeping the young users connected to their parents, it can also be a source of danger and concern for parents. Hence, safer browsing habits need to be nurtured earlier among them. Cybersecurity awareness training was conducted to deliver the content to the targeted group. The objectives of this study are to examine cybersecurity awareness after the participants have gone through the training, to improve a better understanding on cybersecurity awareness and finally to promote safer browsing habits. The cybersecurity awareness is important to develop a good digital citizenship among the young generation. The content of the training includes topics on cybersecurity threats such as pornography, pedophilia, online games addiction and cyberbully. Pre and post surveys have been conducted during each training session. The results show that cybersecurity awareness training is one of the significant ways to increase knowledge regarding cybersecurity awareness starting at a young age. Hence, the finding supports that cybersecurity awareness must be encouraged among the young generation to develop a good digital citizen.

Keyword: Training, cybersecurity awareness, safer browsing habits, digital citizenship,

Introduction

The growth of digital communication and information technology during the last decade has drastically increased. The consequence of this phenomenon is the use of information communication technology (ICT) worldwide and become the most preferred method of interacting and communicating. The unprecedented growth in communications and mobile technology leads to increase the use of mobile devices such as smartphones, tablets and notebooks, most of which are connected to the internet. While such advances in technology have improved communication and access to information, these info structures came along with the risk to the wellbeing of our generation (Mubarak, 2015). As the Internet becomes highly accessible, the issue related to cybersecurity become a matter of concern. Therefore, it is important for us to nurture awareness on what are do's and don'ts while they are online especially among the young generation to promote a safer browsing habit which ultimately will deliver a good digital citizen.

Cybersecurity covers a very broad topic. The concept of cybersecurity, computer ethics, cyber safety, cybercrime, and cyberspace are interrelated with each other. As Malaysia is moving

forward to embrace industrial 4.0, cybersecurity becomes the most important topic to be focused (The Star, 2018). The researchers highlight that cybersecurity is the body of technologies, processes and practices which are designed to protect networks, computers, programs and data from attack, damage or unauthorized access (Khidzir et al., 2016). There are many security approaches that have been taken to tackle cybersecurity challenges such as cryptography, filtering software and network security. Most of the actions taken are mainly on technological matters. Many earlier studies focused on law and enforcement agency tools in combating cybercrime (Juriah & Mahyudin, 2017). However, researchers emphasize that cybe rsecurity is not just about technology and systems but must also take into consideration on the people and processes that rely on the systems (Brian et al, 2011). Considering that the human factors and behaviour can be exploited, this study will explore the impact of training on cyber security awareness.

The objectives of this study are:

1. to examine cybersecurity awareness through training.
2. to improve a better understanding on cybersecurity awareness.
3. to promote safer browsing habits.

The issues of cybersecurity are important as it concerns many users especially young users. A study had found that many users do not undertake a broad range of actions to protect themselves to the threats on the Internet (Cybersecurity, 2014). The pervasive use of digital devices in the country, as well as greater Internet mobility gives more access to the Internet every day. It is reported that the number of Internet users in Malaysia is about 25.08 million which represent 78.79% out of the total population (Hootsuite, 2017). For this reason, there is a need to nurture cybersecurity awareness among Internet users as regards the misused may bring a negative impact to many people. Frost & Sullivan today released the results of its study that the potential economic loss in Malaysia due to cybersecurity incidents can hit a staggering US$12.2 billion (Microsoft, 2018). A high-level awareness on cybersecurity will decrease the occurrences of cybercrime and eventually will promote a good and safer browsing habits.

The cybersecurity awareness training program can be conducted outside of the formal education system. Cybersecurity education, the out-of-class learning approach could help the students to attain several valuable learning outcomes (Kam, 2019). The foundation level of training should be given to the communities to spread underpinning knowledge on cybersecurity awareness.

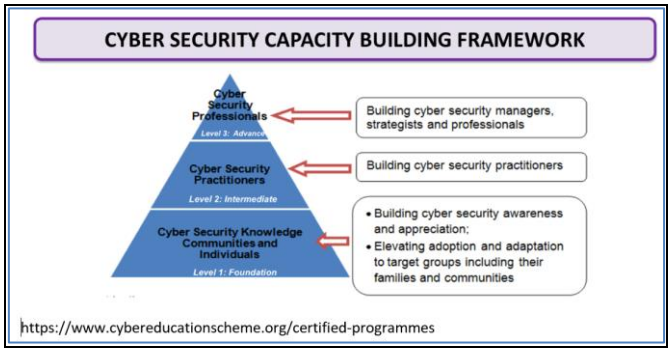

Figure 1 Level of cybersecurity training program (https://www.cybereducationscheme.org/certified-programmes, 2020)

Lack of cybersecurity awareness may expose the Internet user to numerous risks. Some people ignorant of the need to protect themselves while online. One of the risks is the exposure of personal information such as real name, identity card number, address and phone number. The disclosure of personal information may cause illegal usage of the information by somebody who has bad intentions. The online published information can be easily abused by stalkers and crooks, bullies, or even friends. The consequence of the abusing of personal information may disturb the personal life of an individual and lead to a bad impact on children such as being kidnap. These misused of personals information also provide opportunities to third parties to take advantages and use it without asking permission from the owner. They use the information for their different business purposes such as online advertising, customer segmentation, data mining, direct communication and online advertising (Rafique, 2017). Sharing personal information online among children may expose them to be exploited.

Cyberbully is one of the online threats to Internet users especially the young users. The rapid advancement of the Internet and ICT devices has opened a new and infinite space that users can explore with fewer restrictions. Thus, the Internet seems to offer opportunities to humiliate, bully, or harass someone online. The new communication technology has forced people to change the way they behave, and any conflicts between each other have turned into dangerous encounters. To make it worst, a lack of relationships with parents will plunge children deeper into harmful effects of the internet. Consequently, they exposed themselves to the various forms of online bullying including exposure to harassment, flaming, denigration, exclusion and cyberstalking. In some extreme circumstances, those unmonitored behaviors may lead victims of cyberbullying to severe mental illnesses and the worst when it ends with taking their own life (Yusuf et al., 2018).

Materials and Methods

The content of the training namely Modul Bijak Siber was design based on DIGI CyberSAFE National Survey 2013, 2014 and 2015. The survey was conducted by Cybersecurity through a strategic partnership between the Ministry of Education, Cybersecurity Malaysia (CSM) and DIGI Telecommunications (DIGI). The module is then used during the field study for data collection. The training was conducted at three schools and a kindergarten. The duration of each session was about four hours. The session starts with completing a set of pre-program questionnaire. The researchers then gave briefing and explanation about issues related to cybersecurity. After that, the pupil involved in an interactive session using interactive infographics. The infographic contains brief information on the cybersecurity issues and a set of erasable quizzes. Pupils in a group of five members will be doing some activities using interactive infographics such as answering quizzes, completing crossword puzzle. Next, the researcher discussed the appropriate answer with them. After that, the pupils participated in a cybersecurity snake n ladder game using a giant snake and ladder canvas. At the end of the session, pupils were required to answer the post program survey. The questionnaire was adopted from DIGI CyberSAFE National Survey. The question is organized in Bahasa Melayu to cater to various social levels of the respondents. The convenient sampling method was applied in the data sampling technique. Data was collected from 67 respondents who participated in the training. The respondents are standard six pupils from 4 different schools in Machang.

Results and Discussion

The respondents were guided to answer the pre and post questionnaire during the training. Therefore, the response rate is 100%. The result analyzed and the frequency of response calculated. The data type for the study is nominal data. Measurement scale used to portray the result is frequency. Data analyzed by using SPSS. **Table 1** shows the result of the study. The

result shows a significant difference between pre and post questionnaire. The difference depicts that when they have knowledge on cybersecurity issues and threats, then, they know what they should do and should not. The finding of the study describes that if they have knowledge, they will know how to react while they are online. The knowledge gained during the training improved their awareness on cybersecurity.

Table 1 Result of Pre and pro program questionnaire

No.	Question	Pre %	Post %
1.	Saya akan mendedahkan maklumat peribadi saya semasa chatting di Internet	Ya 0% Tidak pasti 12% Tidak 88%	Ya 0% Tidak pasti 3% Tidak 97%
2.	Saya akan memberitahu ibubapa saya sekiranya saya mengahadapi sebarang masalah di Internet	Ya 61% Tidak pasti 28% Tidak 10%	Ya 87% Tidak pasti 12% Tidak 1%
3.	Saya akan mempercayai rakan online saya	Ya 12% Tidak pasti 61% Tidak 27%	Ya 3% Tidak pasti 19% Tidak 78%
4.	Saya akan menghantar gambar kepada orang yang tidak saya kenali melalui Internet	Ya 2% Tidak pasti 7% Tidak 91%	Ya 0% Tidak pasti 1% Tidak 99%
5.	Saya akan membalas mesej yang mengejek saya	Ya 23% Tidak pasti 40% Tidak 37%	Ya 3% Tidak pasti 24% Tidak 73%
6.	Saya akan menggunakan Internet selama mana yang saya suka	Ya 35% Tidak pasti 31% Tidak 33%	Ya 18% Tidak pasti 16% Tidak 66%
7.	Saya akan mendedahkan kata laluan Internet saya	Ya 0% Tidak pasti 15% Tidak 85%	Ya 0% Tidak pasti 0% Tidak 100%
8.	Saya akan memuat turun sebarang kandungan dari Internet	Ya 21% Tidak pasti 51% Tidak 28%	Ya 0% Tidak pasti 34% Tidak 66%
9.	Saya akan menghantar sebarang mesej sesuka hati	Ya 0% Tidak pasti 15% Tidak 85%	Ya 0% Tidak pasti 4% Tidak 96%
10.	Saya akan membantu keluarga saya menggunakan Internet dengan baik	Ya 76% Tidak pasti 22% Tidak 2%	Ya 94% Tidak pasti 6% Tidak 0%

The most significant finding can be seen on question number 5 as shown in **Figure 2**. The cybersecurity threats in the question is regarding replying inappropriate message. In the preprogram survey, majority of the respondents are not sure what they should do if they receive any kind of negative message that annoying them. After went through the training, the majority of them agreed that they should not reply to the message.

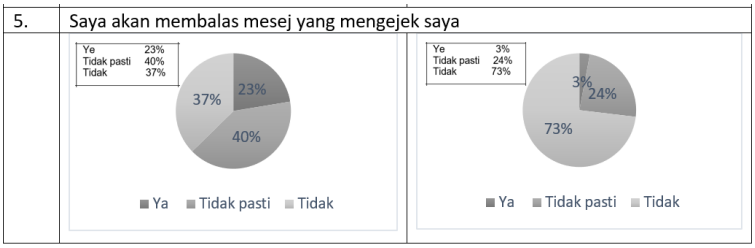

Figure 2 Result for question 5

The other significant finding was portrayed by the result for the question number 3. The result in **Figure 3** shows that most of the respondents did not sure whether they should trust their online friends. After they participate in the program, then they realize that they should have several limitations while dealing with online friends.

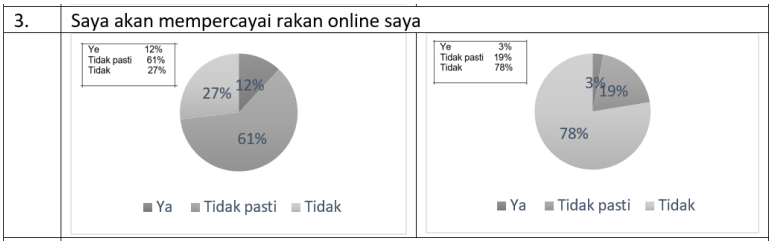

Figure 3 Result for question 3

Most of Internet users do not aware on the downloading activities. As shown in **Figure 4**, before training most of the participant believes that they can download any materials they like. However, after gaining the knowledge during the training they realize that they should mindful of their downloading activities.

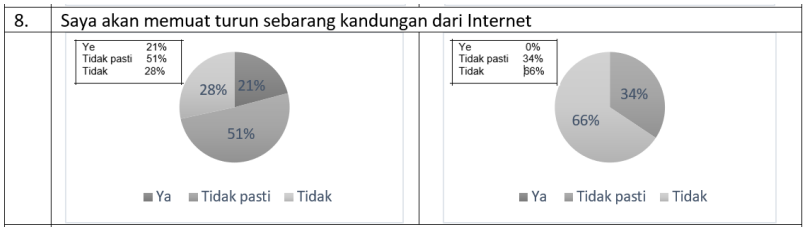

Figure 4 Result for question 4

Modul Bijak Siber was used in this study to deliver cybersecurity concepts and issues. The module contains notes, infographic posters, games, activity book and interactive quizzes. By using the materials, the respondents can visualize the concept and issues on cybersecurity. Therefore, these modules can help participants to get a better understanding on the complex content. The result of the study reveals that the level of cybersecurity awareness among the respondent is raising after they go through the program. For the first question in the pre-program survey pertaining personal information, some of them feel that the personal information can be shared with anybody on the Internet. At the end of the program, then they know that they cannot reveal their personal information. Sharing information on the Internet through any platform may expose them to a serious problem.

The study shows that some of our children are not ready to share with their parents when they are facing any problem while online. Since they are still young and not matured enough, sometimes they may take the wrong way and action to overcome any problem. That is why children must always be guided while online. Without proper guidance from parents and teachers the children tend to believe their online friends.

Another significant finding of the survey is regarding inappropriate action when receiving massages. Some of the respondents believe that they may reply to any message that annoying them. This action should be avoided because it will lead to other problem such as cyberbully. What they are supposed to do is to delete the message and tell their parents or teacher.

Besides that, the result of the survey depicts that our younger generation does not properly guided on how to use the internet. The degree of parental control for the Internet used is not extensive. For example, in terms of Internet usage duration, parents should strictly put a limitation on how long their children can online. Parents also must aware of what kind of web

pages and applications that their children use. The proper monitoring and supervision by adults is important to reduce the misuse of the Internet. Thus, eventually will help our young generation to become a good Internet user and be a good digital citizen.

Conclusion

In the era of hyper-connectivity, children grow up in the environment where people and things are increasingly interconnected digitally anytime and anywhere. It is, therefore, crucial for parents and educators to guide children throughout their online journey. Hence, cybersecurity training is one of the initiatives to nurture cybersecurity awareness. Thus, eventually will help our young generation to become a good Internet user and be a good digital citizen.

Acknowledgement

This article is published as an extension of the ARAS Grant Research (600-IRMI/ DANA 5/3/ARAS (0148/2016). The authors would like to acknowledge IRMI UiTM Shah Alam and PJI UiTM Cawangan Kelantan for the funding.

Conflict of interests

The authors declare there is no conflict of interest with any party in this study and publishing this article.

References

Balakrishnan, V. (2015). Cyberbullying among young adults in Malaysia: The roles of gender, age and Internet frequency. *Computers in Human Behaviour*, 46, 149-157

Brian, M. B., Ramaswamy, D., & Salvatore, S., (2011). Measuring the Human Factor of Cyber Security. IEEE *International Conference on Technologies for Homeland Security (HST)*

CyberSecurity (2013). A National Survey Report 2013. *Safety net: growing awareness among Malaysian school children on staying safe online CyberSecurity of Malaysia.* https://digi.cybersafe.my/files/article/ DiGi_Survey_Booklet_ COMPLETE.pdf [4 December 2019]

CyberSecurity (2014). A National Survey Report 2014. *Safety net: Capacity Building among Malaysian school children on staying safe online*. https://digi.cybersafe.my/files/article/ DiGi_Survey_Booklet_ COMPLETE.pdf. [4 December 2019]

CyberSecurity (2015). A National Survey Report 2015. Growing digital resilience among Malaysian school children on staying safe online. https://digi.cybersafe.my/files/article/ DiGi_Survey_Booklet_ COMPLETE.pdf. [4 December 2019]

CyberSecurity Malaysia (2011). "Children and teenagers exposed to negative cyber culture". *Bernama News*. http://www.cybersecurity.my/en/knowledge_bank/news/2011/main/detail /2087/index.html. [4 December 2019]

Global ACE Scheme. (2020). Certified Programmes. https://www.cybereducationscheme.org/ certified-programmes. [10 February 2020]

Hootsuite. (2017). Digital in Southeast Asia. https://www.slideshare.net/wearesocialsg/digital-in-2017-southeast-asia. [8 December 2019]

Kam, H. J, & Katerattanakul, P. (2019). Enhancing Student Learning in Cybersecurity Education Using An Out-of-Class Learning Approach. *Journal of Information Teknology Education: Innovation in Practies. 18,* 29-47.

Juriah, A. J. (2015). Combating Child Pornography in Digital Era: Is Malaysian Law Adequate to Meet the Digital Challenge?. *Pertanika Journal of Social Science & Humanities*, *23* (S). 137-152

Juriah, A. J., & Mahyuddin, D. (2017). Protecting Children against Exposure to Content Risks Online in Malaysia: Lessons from Australia. *Malaysian Journal of Communication, 33*(1), 115 -126

Khidzir, N. Z, Ismail, A. R, Daud, K. A. M., Afendi, M. S., Ghani, A., & Ibrahim, M. A. H. (2016). Critical cybersecurity risk factors in digital social media: Analysis of information security requirements. *Lecture Notes on Information Theory*, *4*(1), 18-24.

Microsoft, (2018). Cybersecurity threats to cost organizations in Malaysia US$12.20 billion in economic losses. https://info.microsoft.com/ww-landing-Security-Intelligence-Report-Vol-23-Landing-Page-eBook.html/ [13 Ogos 2019]

Mubarak, A. R., (2015). Child Safety Issues in Cyberspace: A Critical Theory on Trends and Challenges in the ASEAN Region. *International Journal of Computer Applications, 129* (1). 49-55

Rafique, G. M. (2017). Personal Information Sharing Behavior of University Students via Online Social Networks. *Library Philosophy and Practice (e-journal),* 1454.

The Star. (2018). Embrace technology for future proof businesses.https://www.thestar.com.my/ [10 Januari 2020]

Von. Solms. R, & Von. Solms. S. (2017). Digital Wellness: Concepts of Cybersecurity Presented Visually for Children. *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance*, 156-166.

Yildirim, S., Celi E., & Yildirim, G. (2016). A Study On The Development of An Infographic Reader Questionnaire And Reader Opinion. *SHS Web of Conference*, *31*.

Yusuf, S., Hassan, M. S., Abu Samah, B., Ibrahim, M. S., Ramli, N. S., A Rahman, N. A., & Osman, M. M. (2018). Parental Attachment and Cyberbullying Experiences among Malaysian Children. *Pertanika Journal of Scholarly Research Review*, *4*(1), 69-80.