Manuscript Submitted	27.09.2021
Accepted	28.12.2021
Published	31.12.2021

Descriptive Analysis: The Impact of Online Cyber Awareness Workshop on Teenagers' Knowledge Of Cyber Issues

Shahrina Binti Shahrani, Wan Fariza Paizi@Fauzi, Suhaila Zainudin, Zulaiha Ali Othman & Khairul Akram Zainol Ariffin
Faculty of Information Science & Technology
Universiti Kebangsaan Malaysia
shahrina@ukm.edu.my, fariza.fauzi@ukm.edu.my, suhaila.zainudin@ukm.edu.my, zao@ukm.edu.my, k.akram@ukm.edu.my

Siti Aishah Sahar
Sekolah Menengah Imtiaz Ulul Albab
Melaka
ikhwanmcg@gmail.com

Abstract

Cyberspace is a place where all information is easily accessible, without limits or restrictions. Anyone, regardless of age, can freely navigate the cyberspace, including teenagers. This study was conducted to investigate teenagers' knowledge about certain cyber issues by conducting a workshop on cyber awareness. Due to the Covid 19 pandemic, the cyber awareness workshop was conducted online. The workshop included several modules on cyber issues that had been previously developed. ADDIE model has been used for the module development. This study aims to look at the impact of online cyber awareness workshops on adolescents' knowledge of cyber issues. A total of 50 high school students participated in the study by completing a questionnaire that was administered at the end of the workshop. The results of the study showed that the implementation of this online workshop on cyber awareness had a positive impact on the students' knowledge. The descriptive analysis has shown that all 50 (100%) students agreed that the workshop was successful in increasing their knowledge of current cyber threats and issues. A total of 48 (96%) students agreed that the way the workshop was conducted made it easier for them to understand the issues in cyberspace. A total of 47 (94%) students stated that this workshop provided them with new knowledge about cyberspace that they were not aware of before. Conducting this online workshop is suitable for students, most of whom use the internet for learning purposes in this Covid-19 period, so they are aware of cyber issues.

***Keywords*:** *cyber issues, awareness, security, teenagers.*

1. Introduction

Internet is a network that has a very wide scale. Nowadays, internet has become a necessity for every individual. Internet networks allow every layer of society to explore cyberspace, and they can do various activities in cyberspace. Ahmad et al. (2017) stated that internet usage had increased dramatically in recent years, and most users are teenagers. Cyberspace is a place where everyone can access all information easily without borders and limitations. Various activities can be carried out in cyberspace. All levels of society are free to surf the cyberspace without hindrance, includingteenagers. Many benefits are obtained, such as facilitating the communication process and information

retrieval, and business dealings. In addition, some websites exist for entertainment and social purposes. However, the passion for surfing cyberspace will have negative effects if the users are naïve and lack of awareness and knowledge on existing threats that lurk in the cyberspace. According to Ahmad et al. (2017), internet technology provides space and facilitates the occurrence of cyber threat activities, and most cases involve teenagers.

Teenagers are easily influenced by what they view, hear or experience. They have a very high curiosity and desire to try new things. Nowadays, teenagers spend more time in cyberspace, thus increasing the probability of getting involved with problems and cybercrime. According to Mokhlis (2019), anyone can browse the website without restrictions, download and upload various materials while allowing users, especially teenagers, to be both exposed and vulnerable to immoral conducts. Cyberbullying, information theft, scams, are some examples of cybercrimes involving all age groups and people from all walks of life. Berita Harian (2016) reported that 70% of 6000 secondary and primary school students were involved in cybercrimes. Among the types of cybercrimes involving teenagers are frauds,virus spread, unauthorised access to systems, and so on (Malik & Kamil, 2010). It is due to the lack of teenagers' awareness of current cyber issues. Children and teenagers are the main targets of cyber thieves because they are among the most active in chat rooms, social media, video streaming sites, and online video games (Corron, 2017). According to Renu (2019), cyberbullyinghas been a frequent problem for teenagers in the last five years. Facebook, Instagram, Snapchat, Twitter, WhatsApp, and telegram are among the social media sites that are very popular with teenagers. The misuse of these social sites can trigger various cyber-related issues such as the spread of fake news, cyberbullying, theft of personal information, and so on.

The SIG (Special Interest Group) CyberHack and Ethics has successfully conducted cyber awareness programs through community outreach events under UKM. The program was held in a face to face format and based on the explorace game approach. During this Covid-19 pandemic situation, everyone spent more time online. The new norm makes most of the work to be carried out online, including teaching and learning activities involving school students. Thus, for the past 24 months, students have spent a lot of time online for learning sessions. Students end up spending more time online, on the pretext of learning but at the same time, they have gain more access to online games and various social media site such as Instagram, YouTube, Facebook, etc. Inadvertently, exposing them to cyber issues such as cyberbullying, sharing of personal information, fraud, dissemination of false information, ransomware, and so on. Teenagers are relatively immature in understanding the implications of their activities in cyberspace. Thus, online cyber awareness workshops are the best alternatives in this current situation to provide teenagers with exposure and awareness of cyber issues to avoid falling into cybercrime activities either as perpetrators or victims. This study aims to conduct an online cyber awareness workshop based on the model developed using existing modules and perform a descriptive analysis to investigate the impact of the workshop on the participating teenagers' awareness and knowledge levels on cyber threats and issues.

2. Current Work

a) Cyber Issues

Cyber issues are factors and contributors to cyber threats and crimes. Cyber issues often heard are cyberbullying, information theft, scams, virus spread, and social media. Facebook, WhatsApp, Telegram, and Instagram are among the social media sites teenagers often visit. A social media site is a platform for sharing and searching for information without borders. The properties found on social media include disseminating, displaying, and sharing information to other users in a short period (Salleh et al., 2017). According to Saizan & Singh (2018), inappropriate information sharing invites criminal cases in social media, including cyberbullying, cyber espionage, scams, phishing, and identity theft. These social media sites are the medium most used by cyberbullies because they use fake identities making them difficult to be tracked and they feel free to do unethical things (Mokhlis,

2019).

One of the severe issues nowadays is cyberbullying among teenagers. Cyberbullying is a thing that teenagers highly fear, and teenagers aged 18 and under are more vulnerable to this issue (Renu, 2019). A study by Karsodikromo et al. (2020) found that the problem of cyberbullying among secondary school students is at a high level that is 60% of 322 forms four students involved with cyberbullying. The effects of cyberbullying can cause anger, sadness, and lack of concentration among victims (Samara et al., 2017). Apart from cyberbullying, information theft can also be among the cyber issues that often involve teenagers. The Pew Research Center (2013) noted that social media users comprised of teenagers tend to share various personal information in cyberspace. This behaviour opens opportunities for cybercriminals to steal and use such information. Misuse of social media, unethical behaviour when browsing cyberspace, and lack of awareness of cyber issues, lead to various offences and cyber threats.

b) Cyber Awareness Programs

Cyber awareness programs are becoming a necessity to educate everyone about cyber issues and cyber threats. These programs can help prevent a person from becoming a victim or perpetrator of cybercrimes. Various programs have been conducted with the common goal of increasing cyber awareness and ensuring safety from cyber threats and crimes. Different types of awareness programs can be conducted such as lectures, distribution of posters and campaigns through mass media. Based on the study by Al Shamsi (2019), a cybersecurity awareness program was conducted by the local Ministry of Education, focusing on training and educating students on cybersecurity best practices in using the internet and materials in the form of lectures, videos, and creating awareness posters. The Malaysian Communications and Multimedia Commission (MCMC) has taken proactive steps to raise awareness in the community by launching the "Klik Dengan Bijak (KDB)" campaign. The campaign aims to raise awareness among those who are exposed to the threats of cybercrimes. It is expected that this program will have a good impact and positively influence the use of the internet. Other programs include a game-based training program (Jin et al., 2018) and cybersecurity camps (Smith & Ali, 2019) designed and organized to raise awareness and address cybersecurity risks among youths.

Rahman et al (2020) stated that cyber security education is essential to protect internet users from cyber threats and crimes that are becoming more common. Awareness and education must be provided at the early stage, especially at the school level, to curb cybercrime. However, there are some challenges in implementation which include teachers' knowledge level, lack of expertise, money and resources (Rahman et al., 2020). Also, the type of awareness program conducted should be suitable for the target audience where the participants effectively listen and participate. The findings of a study by Amankwa (2021) show that cyber security education should be done in educational institutions. Television, radio as well as social media should help to convey the importance of cyber security with exciting and interactive elements.

c) Knowledge on Cyber Issues

Teenagers nowadays are a digital generation vulnerable to the use of the internet and gadgets (Shahrina et al., 2020). They like to explore and find information through websites such as Google and YouTube. No doubt they are intelligent. However, they are relatively immature in understanding the implications of their actions and activities in cyberspace. Knowledge of cyber issues is very important. It ensures that they are not exposed to threats and cybercrimes that harm themselves or their families. The results of a study by Zulkifli et al. (2020) found that most respondents were aware of cyber threats and risks but not many took online security measures due to lack of exposure to the effects and implications of online activities. A study by Ozdamli (2019) also obtained similar results whereby the teenagers knew the general concepts of computer and network security but did not know

specific concepts such as password hacking and remediation actions when exposed to viruses. However, a study by Agbeko (2021) found that teenage cybersafety awareness in Ghana is very high, yet there are still teenagers involved (as criminals) in cyberattacks to generate money and for fun. The lack of exposure to the implications and effects of these online actions leads to the current situation.

3. Methodology

The study commenced with the selection of topics and the production of modules for the selected cyber issues and target audience. Nine main topics of the module were selected based on the current cyber threats: social media threats, cyberbullying, online game addiction, information privacy, think before post, clickbait, virus threats, online shopping, and passwords.

These modules were developed based on the ADDIE model introduced by Rossett (1987). Modules developed based on the ADDIE model are suitable for either online or face-to-face environments (Nada Aldoobie, 2015). The use of this model can produce more effective and efficient learning materials (Stapa, 2019). There were five phases of ADDIE model involved in developing the modules: analysis design, development, implementation, and evaluation. Figure 1 below shows the ADDIE model used in the module development.

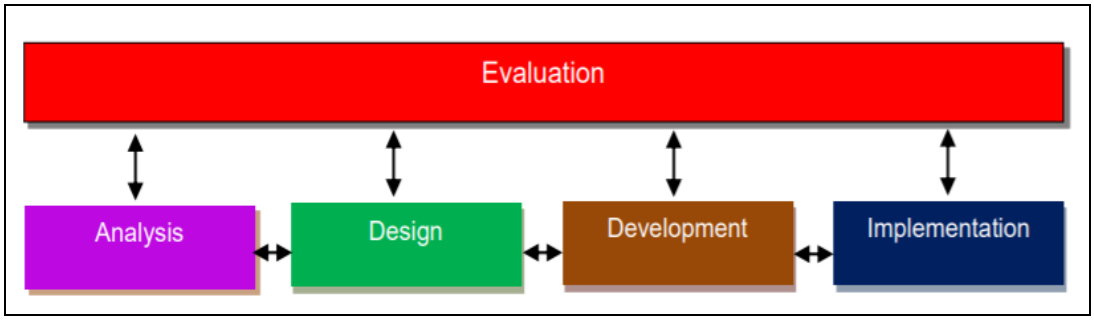

Figure 1: ADDIE Model

(Source: The Use of Addie Model for Designing Blended Learning Application at Vocational Colleges in Malaysia, 2019)

A workshop implementation model were also proposed according to the suitability of the current pandemic Covid-19 situation which required the workshop to be conducted online. The workshop was implemented using the Zoom online platform and the breakout room function. The breakout room function was used to break down the participants into smaller groups and facilitate monitoring throughout the workshop. Figure 2 shows the implementation model of the online cyber awareness workshop used.

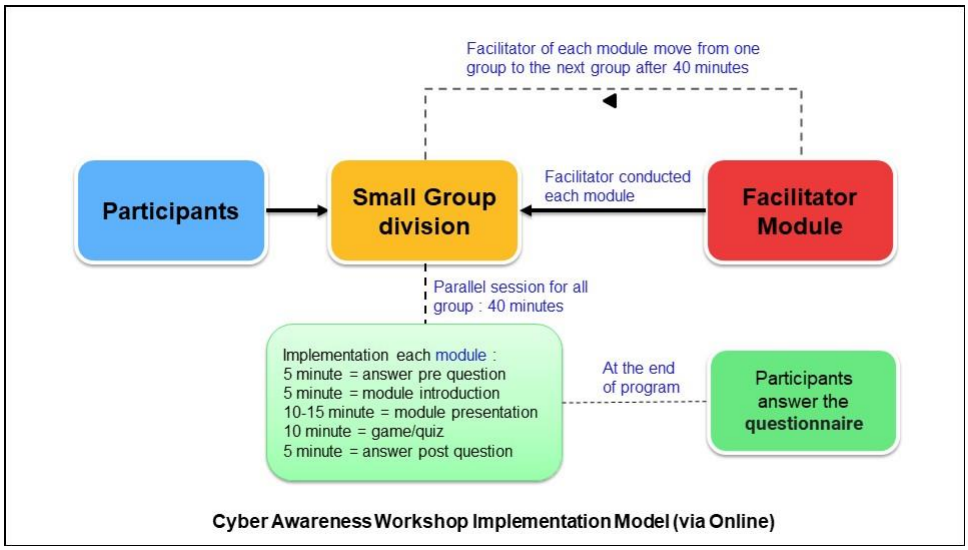

Figure 2: Cyber awareness workshop implementation model

Based on the diagram above, participants were divided into nine small groups and put into nine breakout rooms referring to the nine modules prepared. The facilitator for the module handled each breakout room. Each breakout room was ran in parallel but differs in terms of module. The workshop started with participants answering pre-module questions. Then, the facilitator began to conduct the workshop by introducing the module, presenting the module using infographics slides and videos. The workshop continued with a module reinforcement session where the method used was interactive quizzes or games. Participants collaborated and communicated with group members throughout the session. At the end of the session, participants were given time to answer post-module questions. Each module session took 40 minutes. After completing a module session, the module facilitators moved to another breakout room to continue the workshop while participants remained in their respective breakout rooms.

Figure 3 shows the details of the implementation of the online cyber awareness workshop. With this rotation, participants in each breakout room will attend all nine modules provided. The facilitators moved from one breakout room to the next and conducted their module sessions. The movement of the facilitators continued until all breakout rooms were completed.

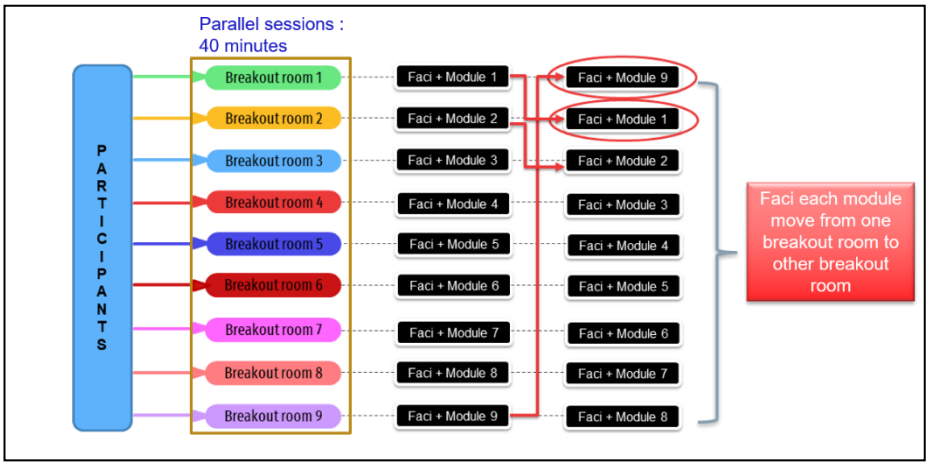

Figure 3: Details of workshop implementation

Figure 4 shows one of the modules used in this online cyber awareness workshop during the introductory session. Each module provided a presentation slide in an infographic and accompanied by a video related to the module title.

Figure 4: Infographic slide module

Figure 5 shows an example of an interactive activity used in the reinforcement session to assess participants' knowledge of the modules described. This activity involved all group members in the breakout room. Participants needed to work together to make this activity a success. This activity required participants to recall all the important contents of the module.

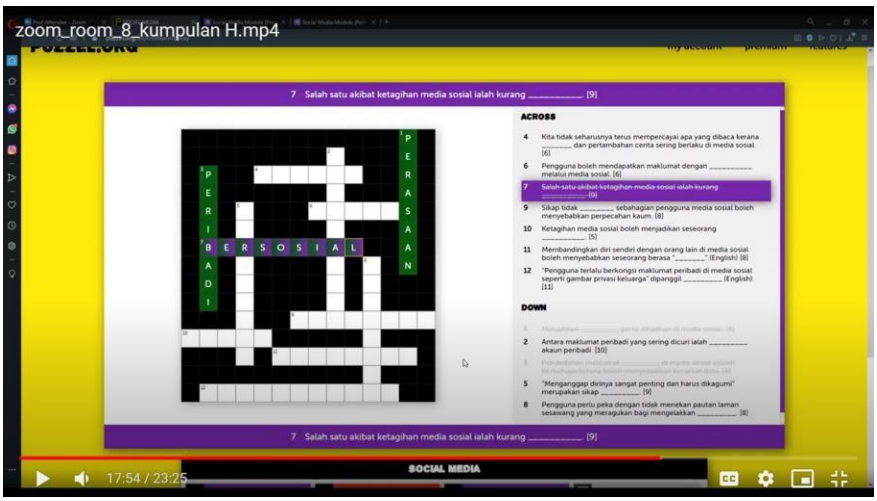

Figure 5: Interactive activity for the module

4. Finding & Discussion

The descriptive analysis of this study focuses on male teenagers from high school students. The results of this study cannot generalize the cyber knowledge of all teenagers in Malaysia but can be an indicator of the teenagers' knowledge on cyber issues.

The participants of this study are 50 Form 4 students from one of the secondary schools in Melaka who completed the online workshop. Questionnaires were given to students at the end of the workshop to get feedback on the cyber issueliteracy and new knowledge in cyber issues as well as to measure the effectiveness of the conducted online workshop.

4.1 Demographic Analysis

Based on figure 6, all 50 respondents were male students. The study involved collaboration from a secondary school in Melaka where all the students are male.

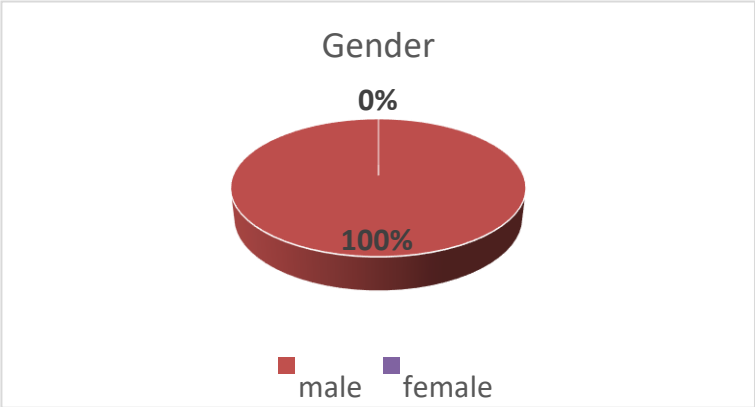

Figure 6: Percentage of respondents according to Gender

4.2 Cyber Issue Literacy

Figure 7 shows that a total of 50 (100%) students agreed that the online workshop conducted successfully increased their knowledge of current cyber threats and issues. The modules used in this workshop cover current cyber problems that often occur in the community. Each module presented includes definitions, objectives, factors that cause a cyber threat, effects, and tips to avoid becoming victims and perpetrators of the issue. A clear description of each issue adds to the students existing knowledge.

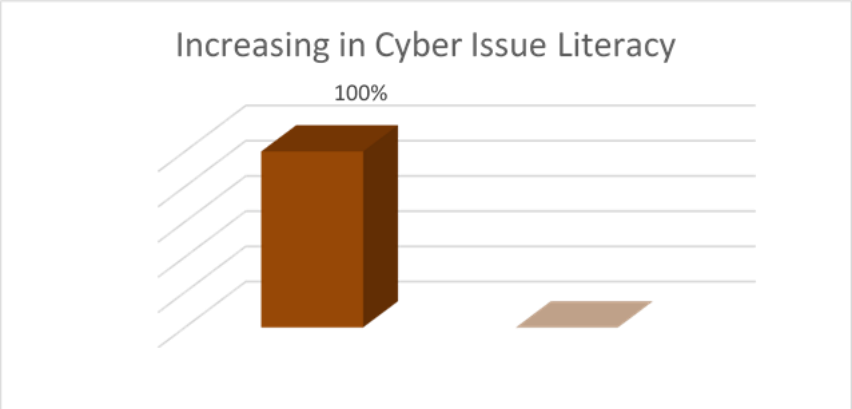

Figure 7: Percentage of respondents according to feedback on their existing cyber issueliteracy improvement

4.3 New Knowledge of Cyber Issue

Figure 8 shows a total of 47 (94%) students who stated that this workshop provided new knowledge related to cyberspace that was not known to them before. There are some cyber issues and threats

that students never knew before were revealed to students in this workshop. Through this workshop, students gained new information on cyber issues and threats that they never knew existed. This can help them to be more careful when surfing cyberspace.

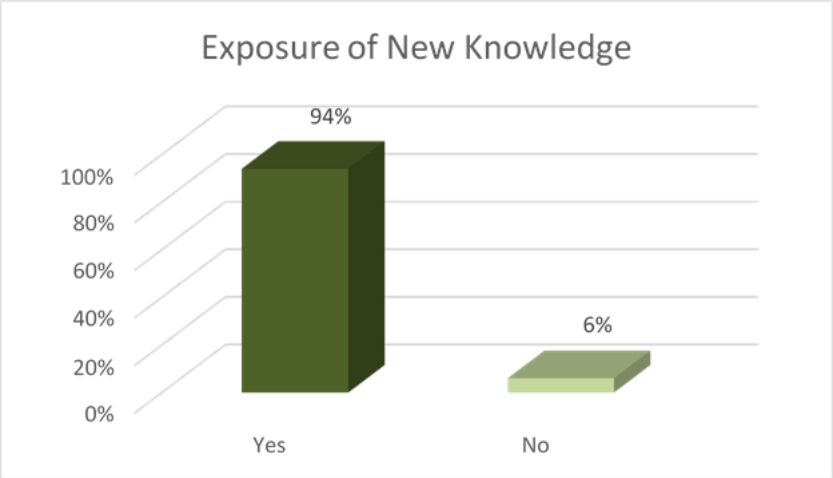

Figure 8: Percentage of respondents according to their feedback on new knowledge of the cyber issue

4.4 Effectiveness of workshop

Meanwhile, based on figure 9, a total of 48 (96%) students found that the material used in implementing this cyber awareness workshop made it easier for them to understand the issues and threats in cyberspace. The workshop was conducted online and in small groups, thus, making it more focused. Each module was provided with infographic presentation slides, videos, and interactive reinforcement activities (quizzes or games) at the end of each issue. The use of infographics and interactive elements of the activity is beneficial for students, especially the current generation nowadays. It is easier for them to understand and focus on visual and interactive material. As a result, at the end of the workshop students were able to answer the quiz correctly.

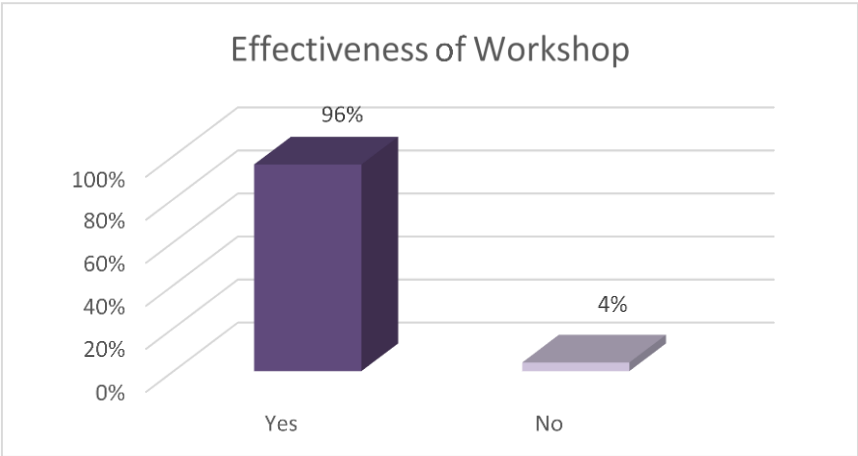

Figure 9: Percentage of respondents according to their feedback on the effectiveness of the implementation online cyber awareness workshop

Based on the results of the analysis, the online cyber awareness workshop had a very positive impact on students. The implementation method of this workshop helped in providing exposure related to cyber issues and increasing students' knowledge also awareness about cyber threats during this pandemic Covid-19 situation. The approach used in the presentation of each module facilitated

students' acceptance of the information presented.

5. Discussion and Future Recommendation

The result of the analysis shows that the online workshop on cyber awareness has an impact on teenagers' knowledge about cyber issues. Cyber awareness among students, especially teenagers, is very important, especially in an era where technology is prominent, and the Internet has become indispensable in daily life. Previous studies have shown that teenagers are most often involved in cases of cyberbullying. To prevent them from getting involved in cybercrimes, they should be educated and made aware at an early age. They need to know and be aware of the current cyber issues and threats in order to reduce the number of cybercrime cases, especially when teenagers are involved. With the availability of cybercrime awareness programs, everyone can learn about it and be sensitized. The awareness and knowledge they gain indirectly will make them protect themselves proactively and increase their ethics so as they do not become the perpetrators in cyberspace. It is hoped that further studies can be conducted to examine the impact and relationship of online workshops in raising awareness among youth.

6. Conclusion

This study found that the workshop provided students, especially teenagers, with insights and increased knowledge on today's cyber issues and threats. The online cyber awareness workshop has positive effects and impact on the students. In conducting the workshop, the small groups facilitated concentration and absorption of the information imparted. Modules presented in the form of infographics and videos and reinforcement units in the form of interactive games/quiz activities used for each module also facilitated absorption of information, increased understanding and knowledge related to cyber issues. This online cyber awareness workshop can also be applied to adolescents in other schools and in different areas such as urban and rural areas, especially in this pandemic Covid 19 situation. This study has some limitations which are the limited number of respondents, covers only one gender namely the form 4 male students and lastly, this study focused only on a certain school.

Acknowledgement

Appreciation to the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia and the management of Sekolah Menengah Imtiaz Ulul Albab, Melaka. This study was carried out under the research grant of Dana Tranformasi Komuniti P&P FTSM with the project code of TT-2020-020.

References

Agbeko, M. (2021). UNDERSTANDING CYBER SAFETY BEHAVIOR AMONG TEENAGERS IN GHANA. *International Journal of Computer Science and Information Security (IJCSIS), 19*(6).

Ahmad, N., Arifin, A., Asma'Mokhtar, U., Hood, Z., Tiun, S., & Jambari, D. I. (2019). Parental awareness on cyber threats using social media. *Jurnal Komunikasi: Malaysian Journal of Communication*, 35(2).

Al Shamsi, A. A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. *International Journal of Information Technology and Language Studies, 3*(2),8-29.

Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security*, *12*(4), 233-249.

Branch, R. M. (2009). *Instructional design: The ADDIE approach* (Vol. 722). Springer Science & Business Media.

Corron, L. (2018, January). Social Cyber Threats Facing Children and Teens in 2018. Retrieved from November 5th, 2018 from https://staysafeonline.org/blog/social-cyber-threats-facing- children-teens-2018/ .

Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018, February). Game based cybersecurity training for high school students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (pp. 68-73).

Karsodikromo, Y., Husin, M. R., Razali, A. R., & Hamzah, H. (2020). Buli siber dalam kalangan murid sekolah menengah di daerah Samarahan, Sarawak. *Jurnal Pendidikan Bitara UPSI*, *13*(2), 38-47.

Malek, M. D. A., & Kamil, I. S. M. (2010). Jenayah dan masalah sosial di kalangan remaja: cabaran dan realiti dunia siber.

Mokhlis, S. (2019). BULI SIBER DALAM KALANGAN PELAJAR SEKOLAH MENENGAH: SATU PENEROKAAN AWAL. *Jurnal Dunia Pendidikan*, 1(2), 7-18.

Nada Aldoobie. (2015). ADDIE Model. *American International Journal of Contemporary Research*, Vol. 5, No. 6.

Ozdamli, F., & Ercag, E. (2019). Knowledge levels and attitudes toward cybercrimes of adolescentsin Northern Cyprus. *TEM Journal*, *8*(4), 1345.

PewResearchCenter. 2013. Teens, Social Media, and Privacy. The Berkman Center for Internet & Society. Harvard University.

Rahman, 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.

Renu, P. (2019). Impact of Cyber Crime: Issues and Challenges. *International Journal of Trend in Scientific Research and Development (ijtsrd)*, ISSN: 2456- 6470, Volume-3 | Issue-3, April 2019, pp.1569-1572.

Rossett, A. (1987). Training needs assessment. Englewood Cliffs: Educational Technology Publication.

Saizan, Z. A. K. I. A. H., & Singh, D. A. L. B. I. R. (2018). Cyber security awareness among social media users: Case study in German-Malaysian Institute (GMI). *Asia Pac. J. Inf. Technol. Multimed*, *7*, 111-127.

Salleh, M. A. M., Abdullah, M. Y. H., Salman, A. & Hasan, A. S. A. 2017. Kesadaran Dan Pengetahuan Terhadap Keselamatan Dan Privasi Melalui Media Sosial Dalam Kalangan Belia. e-Bangi 12(3): 127 1–15. Retrieved from http://ejournals.ukm.my/ebangi/article/view/22475/7071

Samara, M., Burbidge, V., El Asam, A., Foody, M., Smith, P. K., & Morsi, H. (2017). Bullying and cyberbullying: Their legal status and use in psychological assessment. International Journal of Environmental Research and Public Health, 14, 1-17.

Shahrina Shahrani, Rohizah Abd Rahman, Masura Rahmat, Azura Ishak, Noor Faridatul Ainun Zainal, Hafiz Mohd Sarim. (2020). A Descriptive Analysis of The Implementation Video-Based Module to The Student through Active Learning in Project. *Malaysian Journal of Information and Communication Technology*, Vol 5 2020, Issue 2

Smith, D. T., & Ali, A. I. (2019). YOU'VE BEEN HACKED: A TECHNIQUE FOR RAISING CYBER SECURITY AWARENESS. *Issues in Information Systems*, *20*(1).

Stapa, M. A., & Mohammad, N. A. Z. E. R. I. (2019). The Use of Addie Model for Designing Blended Learning Application at Vocational Colleges in Malaysia. *Asia-Pacific Journal of Information Technology and Multimedia*, *8*(1), 49-62.

Zulkifli, Z., Molok, N. N. A., 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.