SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

# Cybersecurity Awareness among Secondary School Students Post Covid-19 Pandemic

Masita Jalil[1,*] , Noraida Hj. Ali[1], Farizah Yunus[1], Fakhrul Adli Mohd Zaki[1], Lee Hwee Hsiung[2], MA Almaiah[3]

[1] Faculty of Computer Science and Mathematics, Universiti Malaysia Terengganu, Malaysia
[2] CyberSecurity Malaysia, Cyberjaya, Malaysia
[3] Faculty of Information Technology, Aqaba University of Technology, Jordan

**ARTICLE INFO**

***Article history:***
Received 9 May 2023
Received in revised form 19 September 2023
Accepted 2 December 2023
Available online 9 January 2024

***Keywords:***
Cybersecurity; cyber awareness; cyber threats; COVID-19

**ABSTRACT**

The COVID-19 pandemic has significantly transformed the landscape of education delivery, leading to a surge in online teaching and learning methods, and consequently, increased Internet usage among students. These circumstances have created an environment that makes them vulnerable to cybercrime due to the lack of cybersecurity awareness. This paper proposes a cyber-awareness program aimed at increasing students' knowledge of cybersecurity and their ability to manage the risk of cyber threats. The methodology consists of four phases: Initiation and Planning, Development of Modules, Implementation, and Evaluation. The results of descriptive and statistical analyses show an increase in participants' awareness of cyber security threats and risks following their participation in the program. In conclusion, this program has successfully achieved its objectives of enhancing cyber security awareness and promoting safe internet usage among participants. These findings suggest that similar programs can be utilized to increase cybersecurity awareness and promote safe internet usage among students.

## 1. Introduction

### *1.1 Research Background*

COVID-19 pandemic gave rise to significant changes in the delivery methods of teaching and learning activities in Malaysia [1]. The teaching and learning process, which was previously implemented face-to-face, is now adopting the online learning approach. This approach allows teaching and learning sessions to continue by adhering to the standard operating procedures (SOPs) in force to reduce the spread of COVID-19 outbreaks. This new norm in the teaching and learning process has indirectly increased the number of Internet users among students. This is clearly seen from the published findings of the Malaysian Internet Users Data 2020 [2], which shows an increase of 155% in users aged between 5-17 years in 2020 (47%) compared to only 18.4% in 2016.

[*] *Corresponding author.*
*E-mail address: masita@umt.edu.my*

https://doi.org/10.37934/araset.37.1.115127

The Internet has become a new medium of social relations and changing the paradigm of society in many ways. Through the internet, various mass media have come into existence as a medium of social media communication such as Facebook, Twitter, WhatsApp, Instagram, and many more.

Daily use and dependence on the internet and media social technology not only exposes students to new knowledge but also opens the door to increasing cyber threats such as misuse of personal data, cyberbullying, cases of harassment, and fraud. Low cyber awareness among Internet users has been identified as one of the main factors contributing to the increasing percentage of cyber threat cases [3]. As outlined in the Malaysian Cyber Security Strategic Plan 2020-2024, one of the strategic pillars of Malaysia's five-year cyber security plan is to enhance the country's cyber security capabilities, increase cyber awareness among users, and nurture cyber security knowledge through education [3].

To ensure the implementation of the national cyber security plan achieves its goals, CyberSecurity Malaysia (CSM) teams with government agencies and industry players are actively involved in designing and coordinating programs and campaigns to expose and increase cyber security awareness among internet users in Malaysia, especially among students. While such initiatives help in spreading cyber security awareness among kids, youths, and parents, it may not able to reach a wider audience [4].

Gamification refers to the use of game approaches and strategies to engage and increase user motivation in solving specific problems through the application of elements of competition and reward [5]. The concept of gamification is becoming increasingly popular today and its application in corporate training programs is showing positive initial results. Gamification approaches have also started to be introduced in several countries such as the USA, United Kingdom, and Norway to foster and increase cyber security awareness [5-8]. According to a study conducted by Pulse Learning [9], 79% of participants agreed that a more game-like learning environment can increase motivation and productivity levels as well as be able to increase engagement and the effectiveness of training programs.

In Malaysia, the concept of gamification is still relatively new and has not been widely applied in the context of cyber security. The available cyber security awareness training modules can be incorporated with gamification elements to stimulate the interest and involvement of participants, especially students. Thus, a training module that incorporates interactive learning based on the concept of gamification will be designed and developed in collaboration with CSM to increase students' interest and involvement in understanding cybersecurity risks and acquiring the skills to deal with cyber threats.

This paper is organized into four sections. The remainder of Section 1 provides a brief description and review of related literature. Section 2 elaborates on the research methodology while Section 3 discusses the results. Conclusions are later drawn in Section 4 together with directions for future works.

### *1.2 Related Works*

Being aware of cyber security in everyday situations is referred to as cyber security awareness. This includes understanding the risks associated with online interactions through various social media platforms, email, and web surfing [10].

Cybersecurity is becoming increasingly important in today's digital environment. Government, military, commercial, education, and healthcare industries all use technology to collect and store sensitive data and information for various purposes. At the same time, an increase in cybercrime incidents has been recorded [11].

The unpredictable human nature and behavior make people an essential component and enabler of cybercrimes [12]. Previous studies have shown that individuals' ignorance of the threats they may encounter online can lead to the successful implementation of those threats [12]. Therefore, creating a culture of cyber awareness among users has become more important nowadays than ever before.

The adverse risks of the technological revolution in mobile phone and Internet technologies are currently being brought to youngsters [4]. According to reports, as the number of children using the Internet grows, so does their susceptibility to criminal conduct by online predators [4]. The younger generations could be significantly harmed by these cybersecurity vulnerabilities, which include suffering from addiction, cyberbullying, identity fraud, and other problems. The reason for this is that many still could not comprehend cybersecurity, especially the young (those between the ages of 15). The most significant finding of this study is the necessity of increasing youngsters' cybersecurity knowledge. Additionally, the longer children are online, the more likely they are to become victims of cybercrime. According to Garba *et al.,* [14], there is a higher risk for young people who often use the internet incorrectly to find information to satisfy their curiosity. Young people between the ages of 13 and 15 who lack knowledge and understanding of cyber security are the group that usually become easy targets. The younger generations could be significantly harmed by these cybersecurity vulnerabilities, including experiencing addiction, cyberbullying, identity fraud, and other problems. The reason for this is that many still could not comprehend cybersecurity, especially the young (those between the ages of 15). The most significant finding of this study is the necessity of increasing youngsters' cybersecurity knowledge.

Another study by Espinha *et al.,* [15], conducted in an academic institution found that students were reluctant to participate in cybersecurity awareness activities. This study suggests that academic institutions may be able to help raise students' awareness levels by distributing cybersecurity information to them more frequently. Similarly, findings by Potgieter [16] concluded that academic institutions should take the necessary steps to increase students' awareness of cyber security through available communication channels.

Based on a survey conducted by the Malaysian Communications and Multimedia Commission (MCMC), Malaysian internet users spent an average of 6.6 hours online per day in 2018 [2]. The number of Internet users is growing daily due to dependency on information and communication technology (ICT) brought forth by several government initiatives to scale up Internet access, which also significantly alters Malaysia's cyber threat environment [17]. Likewise, the findings of the recently published Malaysian Internet User Survey [1] recorded an increase of 155% of users between the ages of 5-17 in 2020 (47%) as compared to only 18.4% in 2016. The percentage is likely to increase in the period of 2020-2022 following the nationwide implementation of online or home-based learning for schools throughout the period of the movement control order in Malaysia which has been enforced since August 2020 [18].

A recent study by Ng and Kamsin [4] revealed that students in Malaysia are heavily exposed to the Internet. Yunos *et al.,* [19] found that Malaysian students in primary and secondary schools are largely aware of cyber security issues. However, the extent to which they understand the associated cyber security risks and are aware of the appropriate actions to be taken to avoid becoming victims of such crimes is still unclear and requires further research. The prevalence of cases involving internet scams, cyberbullying, online harassment, identity fraud, and other issues is rising daily as a result of the lack of information about the Internet. Hence, younger generations need to be protected because they are highly susceptible to becoming victims of cybercrime [20-22]. In addition to ensuring a safer environment for the next generation of young people, some concerns must also be addressed. According to Yunos *et al.,* [19], as students will be more inclined to use the Internet as they get older and the ways and purposes for which they use the Internet are constantly changing, it is important to continuously expose them to a variety of issues and best practices. While educating children is necessary, educating parents is also important because they act as their children's first "teachers" in safe Internet use.

In summary, research on cybersecurity awareness among students and their level of cybersecurity knowledge is relatively underdeveloped, with the majority of earlier studies concentrating more on technological issues [23]. Our objectives were to investigate cyber awareness levels among secondary school students post-COVID-19 pandemic and offer perspectives on the current status. Our study strategy is mainly focused on examining trends in student behaviors that are related to students' level of cyber awareness. The findings of this study can assist schools in addressing student cyber issues.

## 2. Methodology

### *2.1 Research Design*

This study is conducted to assess the level of cybersecurity awareness among secondary school students in Malaysia before and after attending a cybersecurity program that incorporated interactive activities based on gamification elements. The study aimed to evaluate the effectiveness of the program in achieving its objectives. A total of 165 upper secondary students (age above 15 years old) from five secondary schools in Kuala Nerus district, Terengganu, Malaysia participated in the program. It was offered only to schools that implemented full online or home-based learning. The selection of Kuala Nerus district was a requirement of the grant to ensure that the local communities could benefit from the research.

To measure the effectiveness of the program, pre- and post-program surveys were developed as research instruments. The pre-program survey had two sections, focusing on basic information on social media skills and the participants' level of cybersecurity awareness before being exposed to the program materials. A post-program survey was conducted to gather feedback on the participants' level of awareness after attending the program. The survey items were measured using a Likert scale of 1-5, with 1 indicating very low or strongly disagree, and 5 indicating very high or strongly agree.

Descriptive analysis was performed on the pre- and post-program survey data from only 105 participants who completed both questionnaires, due to missing and incomplete questionnaires submitted by some of the participants. The analysis gave a visual representation of the findings. A non-parametric test for the paired dependent sample of ordinal data type was also conducted to confirm whether there was any significant difference in the mean score before and after the program.

### *2.2 Methodology*

The complete methodology comprises four phases: Initiation and planning, Development of Training Modules, Implementation, and Evaluation. Activities carried out in each phase are as described below.

i. Phase 1: Initiation and Planning
   In this phase, the trainers who will be involved with the cyber security program attended the Cybersecurity Essentials ‘Training of Trainers’ course offered by Cybersecurity Malaysia. This training provides the trainers with enough preparation to conduct the cyber awareness program later. Then, suitable contents for the training modules are identified based on the set target group. Among the modules listed are a) Introduction to Cyber Security, b) Cyber Security Threats and Risks, c) Cyber Bullying, d) Identity Theft, e) Internet Addiction, f) Malware, and g) Internet

Usage Ethics. To ensure effective delivery in the later awareness program, appropriate gamification approaches and elements are added to attract participants.

ii. Phase 2: Development of Training Modules
Upon completion of the first phase, the second phase focuses on the development of training modules. The content of the module is developed specifically for the target group consisting of secondary school students. Module development involves the use of graphic media tools utilizing HTML5 technology that provides an interactive environment. Apart from that, instruments for pre- and post-program surveys are also designed to collect participants' feedback. The results of the feedback will be used in the evaluation phase later.

iii. Phase 3: Implementation
Due to the COVID-19 pandemic situation at the time this study was done, the cybersecurity awareness program was conducted online using the Cisco Webex application. Access by the target group was established through various devices such as desktop computers, laptops, and mobile phones.

iv. Phase 4: Evaluation
This last phase involves an evaluation of the programs that have been carried out. This was done through research instruments and pre- and post-program surveys which were administered to the participants before and after the program. The last activity done for this study was to prepare a report on the results of the study and suggestions for improvement in the future.

## 3. Results and Discussion

The study has two main objectives, namely to assess the perceptions of social media use and to determine the level of cybersecurity awareness among participants. The first part of this section comprises the presentation and discussion of the descriptive analysis of the collected data, while the subsequent section focuses on the results of the inferential statistical analysis conducted on the pre- and post-program survey data to establish any evidence of increased awareness after program participation.

### *3.1 Descriptive Analysis*

### *3.1.1 Perception of social media usage*

The first part of the pre-program survey looked at perceptions of social media usage among participants which cover five items as given in Table 1.

**Table 1**
Social Media Usage Items

| A. Basic Information on Social Media (SM) Usage | |
|---|---|
| A1: | I am knowledgeable in the use of social media despite not attending any ICT related programs or courses. |
| A2: | I am aware of the importance of making privacy settings in social media accounts. |
| A3: | I can distinguish whether the information shared is true or false. |
| A4: | I am aware of who I share information with on social media. |
| A5: | I maintain behaviour and communication throughout using social media. |

Based on the results presented in Figure 1, a total of 22 participants (21%) reported having a very high level of knowledge (score 5) in using social media, while 51 participants (49%) reported a high level (score 4). Moreover, over 80 participants (79%) indicated being aware of the importance of privacy settings on social media accounts. Additionally, 40 participants (38%) perceived themselves as capable of discerning true from false information before sharing it on social media. Furthermore, 72 participants (69%) strongly agreed that they knew the individuals with whom they shared information, and 59% reported maintaining good behaviour while using social media (score 5). Overall, the participants exhibited considerable social media proficiency, despite not having undergone any formal training. Furthermore, more than half of the participants initially demonstrated good social media ethics.

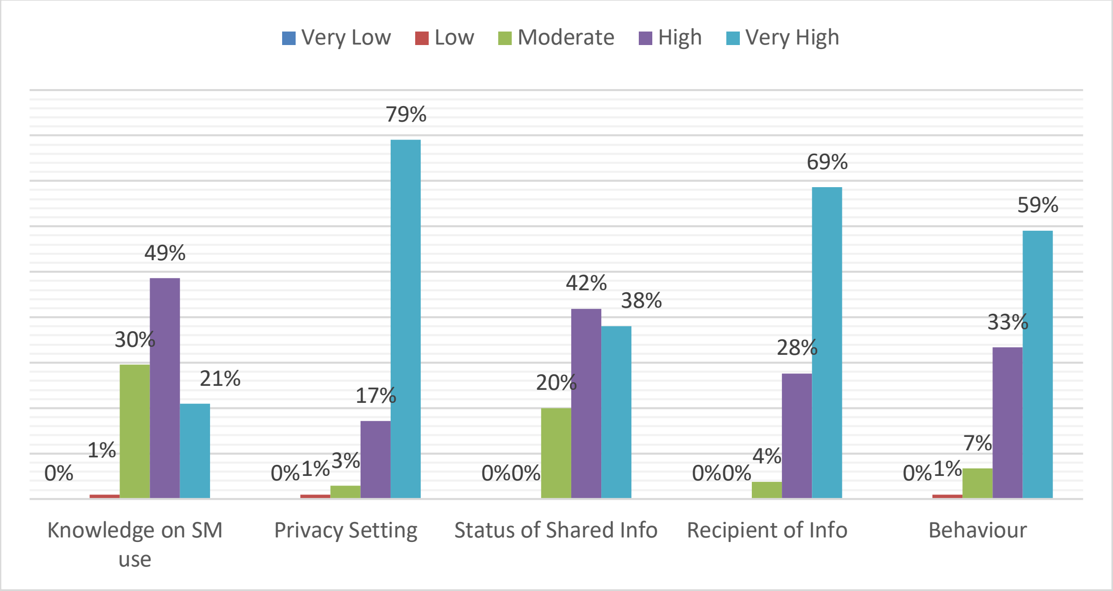

**Fig. 1.** Perceptions of Social Media (SM) Usage

### *3.1.2 Levels of cyber security awareness*

The second part of the pre-program survey assesses participants' levels of cyber security awareness prior to exposure to program contents. While the questionnaire used for the post-program survey gauges the awareness after participating in the program. This included participants' knowledge of cyber risks and threats in general, cyberbullying, identity theft, internet addiction, and viruses/malware. The following subsections detail out the comparison of the pre- and post-program survey findings for each of the cybersecurity concerns.

i. Cybersecurity Knowledge
Based on the findings obtained as illustrated in Figure 2, there was an increase in the level of cybersecurity knowledge among participants after following the program. More than 70% of the participants highly agreed that they were more knowledgeable on cybersecurity compared to only 37% before exposure to the contents. This shows an increase of 34%. More participants knew the meaning of cyber security and were able to score in the interactive activities held.

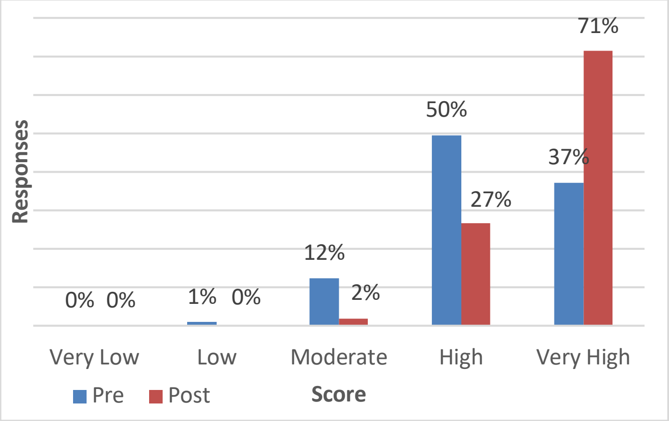

**Fig. 2.** Comparison of results for cybersecurity knowledge

ii. Cybersecurity Threats and Risks

The second survey item assessed participants' overall awareness of cybersecurity threats and risks. Figure 3 presents a comparison of pre- and post-program survey results. The graphical representation indicates that the majority of participants (99%) exhibited a high or very high level of awareness, which is a notable increase from the 82% observed prior to the program. It is also noteworthy that, as anticipated, 51% of participants initially exhibited a low to moderate level of awareness. However, following the program, the proportion of participants exhibiting low to moderate awareness significantly decreased to just 1%.

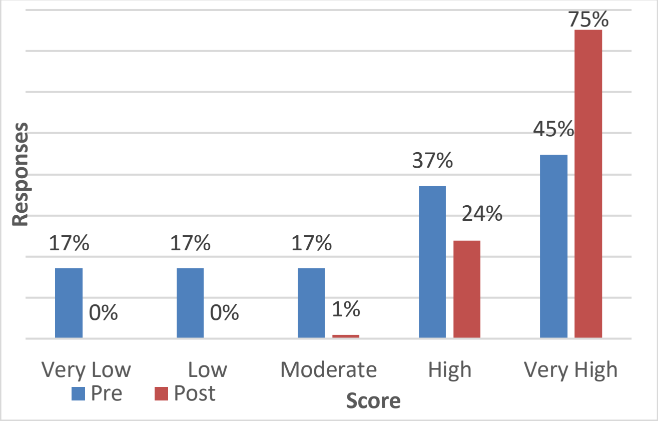

**Fig. 3.** Comparison of results for cybersecurity threats and risks

iii. Cyber Bullying

The post-program survey revealed a significant increase in the proportion of participants who demonstrated a very high level of awareness concerning cyberbullying and strategies to address it. As depicted in Figure 4, 70 (67%) participants exhibited high levels of awareness, representing a considerable increase from the 27 (26%) participants in the pre-program survey, indicating a rise of 61.4%. In general, all participants had moderate to very high levels of awareness after completing the program.

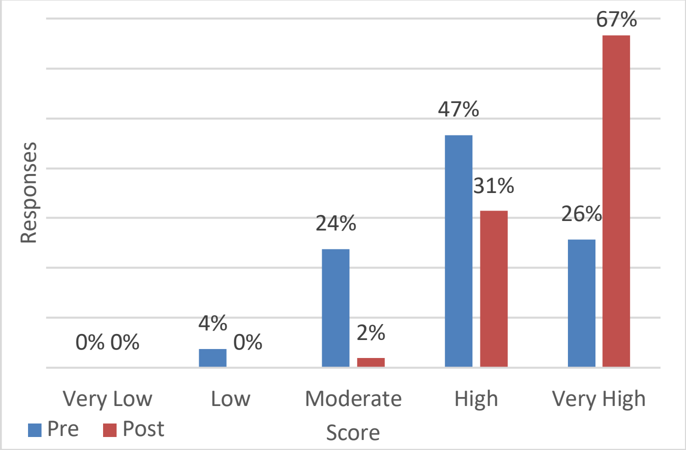

**Fig. 4.** Comparison of results for cyber bullying

iv. Identity Theft

The data shows a significant increase in participants' awareness of the risks associated with identity theft while browsing the Internet (as depicted in Figure 5). Specifically, 73 (70%) participants exhibited a high level of awareness, which represents a 35% increase from the 47 (45%) participants who demonstrated such awareness prior to the program. Importantly, none of the participants exhibited low or very low awareness of this risk following the program.

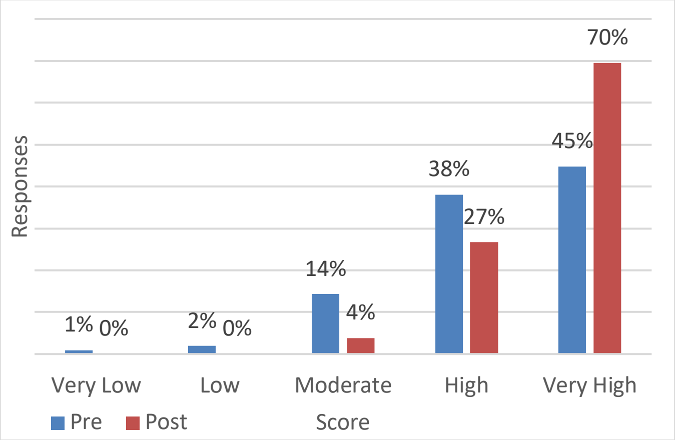

**Fig. 5.** Comparison of results for identity theft

v. Internet Addiction

As for Internet addiction, there was a slight increase in participants' level of awareness on the implications of uncontrolled Internet use as depicted in Figure 6. The percentage of participants who were aware of the risk of Internet addiction increased by 14%, from 70% to 84%. However, one participant felt that his awareness was still at a low level and one at a moderate level, which might indicate that they were less aware of the existence of these risks than before joining the program.

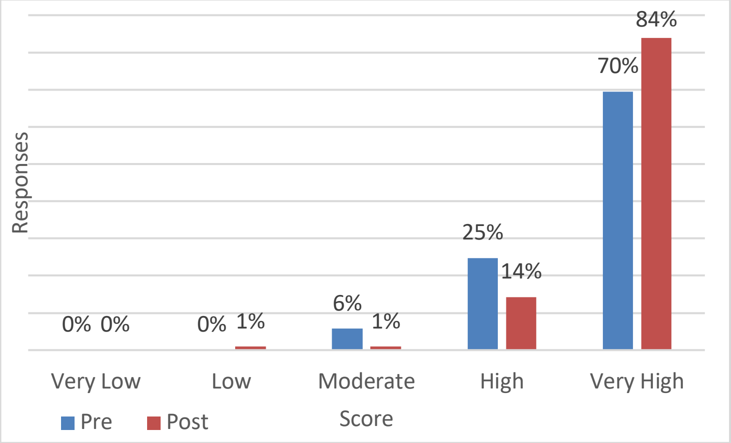

**Fig. 6.** Comparison of results for Internet addiction

vi. Malware (Viruses)

The level of awareness of malware or virus threats also shows an increase of 26%, from 44% to 70%. All participants were more aware that their gadgets could be at risk of being infected with viruses at some point while they surfed the Internet.

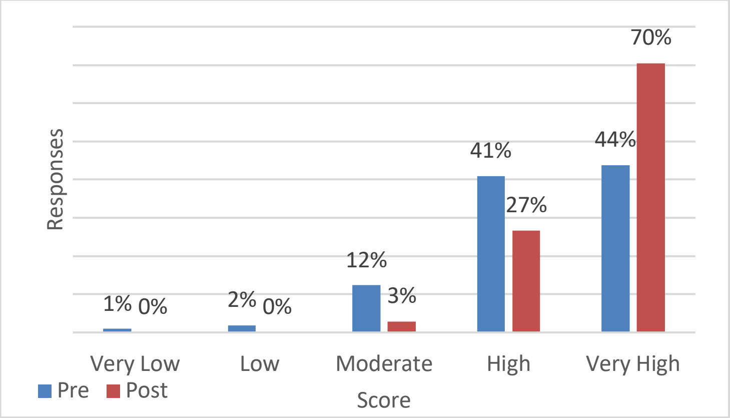

**Fig. 7.** Comparison of results for malware

vii. Ethical Use of the Internet

At the end of the program, an increase was also recorded in the level of awareness of participants on the need to be prudent Internet users to reduce the risk of cyber threats as presented in Figure 8. The majority of participants responded with a score of 4 and 5, indicating that they were more aware. This awareness and responsible attitude are important to ensure a safe and risk-free Internet environment.

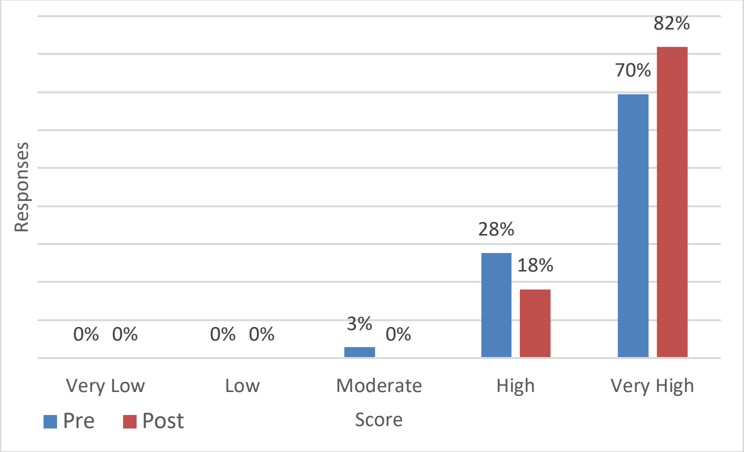

**Fig. 8.** Comparison of results for ethical use of the Internet

The instrument used for the post-program survey also assesses the participants' ability to apply the knowledge gained from the program to help them use the Internet more safely. Based on the results of the study as given in Figure 9(a), it can be seen that 73 participants (70%) strongly agreed with their ability to apply the knowledge gained, while 29% agreed. In terms of the effectiveness of the interactive activities used throughout the course of the program, as depicted in Figure 9(b), 80% of the participants strongly agreed that the activities were very effective in helping them to better comprehend the risks of cyber threats and ways to address them. Another 19% agreed that the activities were effective while one felt neutral. All participants also expressed interest in following similar programs in the future.

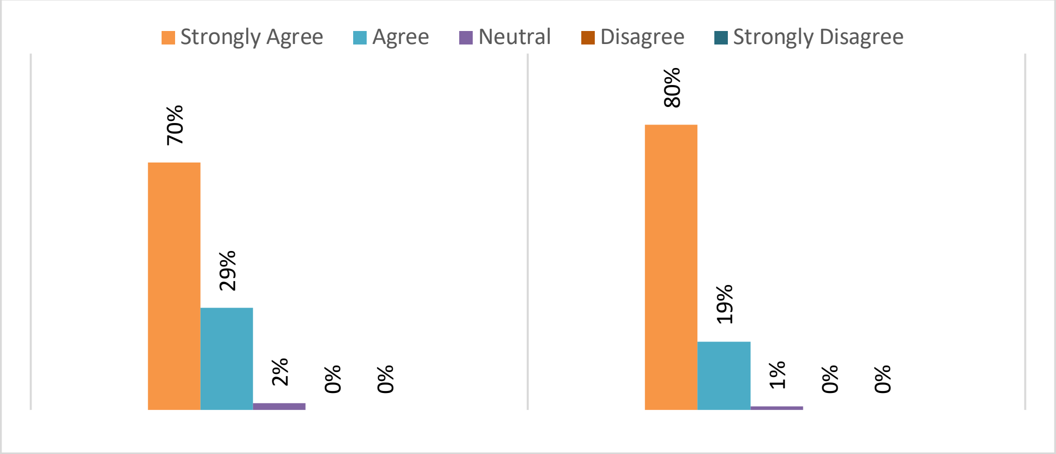

**Fig. 9. (a)** Ability to apply cyber awareness knowledge

**Fig. 9. (b)** Effectiveness of program activities

### 3.2 *Inferential Statistical Analysis*

The second part of this section presents and discusses the results of the inferential statistical analysis performed on the survey data. The inclusion of this analysis is important in order to test the research hypothesis, thus establishing any evidence of increased awareness after program participation. The signed test was suitable for use as the sample comprise of ordinal data types.

The sign test is a nonparametric test that compares the number of positive and negative differences between the before and after results for each individual [24]. The null hypothesis is that the means of the differences (µ1 - µ2) is zero whereas the alternative hypothesis is that the mean of the differences is not zero [25], as given in Equation (1) and Equation (2) respectively.

$$H_0 = \mu 1 - \mu 2 = 0; \tag{1}$$

$$H_1 = \mu 1 - \mu 2 > 0; \tag{2}$$

The variables tested are the awareness of *Cybersecurity Knowledge(v1), Cybersecurity Threats and Risks (v2), Cyber Bullying (v3), Identity Theft (v4), Internet Addiction (v5), Malware (Viruses) (v6),* and *Ethics of Internet Use (v7)*.

Table 2 presents the numbers of positive differences (x), negative differences, and the sample size of each variable. Using the normal-curve approximation for Binomial Variable, X, with p = ½, the test statistics Z and the respective P values obtained are as depicted. Since the P values are greater than 0 for all the variables, the null hypothesis is rejected. This implies that there is a difference in the mean of the samples. In other words, the test statistics confirm that the evidence is sufficient to conclude that based on the sample mean, the awareness level has increased following the program participation.

**Table 2**
Sign test results

| | v1 | v2 | v3 | v4 | v5 | v6 | v7 |
|---|---|---|---|---|---|---|---|
| Positive (x) | 46 | 44 | 60 | 38 | 23 | 41 | 20 |
| Negative | 4 | 4 | 2 | 6 | 8 | 7 | 5 |
| Sample Size (n) | 50 | 48 | 62 | 44 | 31 | 48 | 25 |
| Z value | 5.8 | 5.6 | 7.2 | 4.7 | 2.5 | 4.8 | 2.8 |
| P=P(x≥n)=P(Z>z) | 0.9997 | 0.9997 | 0.9997 | 0.9997 | 0.9948 | 0.9997 | 0.9978 |

## 4. Conclusions

The primary objective of the cybersecurity awareness program was to educate participants on the various cybersecurity risks and threats using the training modules developed. The effectiveness of the program and the level of awareness were evaluated using research instruments. The participants exhibited good knowledge of social media usage and perceived that they were practicing good social media ethics before the program. However, the descriptive and statistical analysis of the pre- and post-program surveys revealed a significant increase in their level of awareness of cybersecurity threats after attending the program. The interactive activities employed during the program were effective in enhancing their understanding of the risks associated with cyber threats and how to address them. Therefore, it can be concluded that the program successfully achieved its objective of increasing cybersecurity awareness among the participants. The program also enhanced their confidence in applying the knowledge gained to become more vigilant and responsible internet users. This outcome suggests that similar programs can be used to increase cybersecurity awareness and promote safe internet usage among the general public.

**Acknowledgement**
This research was funded under the Knowledge and Technology Assimilation Grant Scheme (KTAGS), PPIJI, Universiti Malaysia Terengganu (UMT).

## References

[1] Masrom, Maslin, Mohd Nazry Ali, Wahyunah Ghani, and Amirul Haiman Abdul Rahman. "The ICT implementation in the TVET teaching and learning environment during the COVID-19 pandemic." *International Journal of Advanced Research in Future Ready Learning and Education* 28, no. 1 (2022): 43-49.

[2] Malaysian Communications and Multimedia Commission. (2020), Internet Users Survey 2020, https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/IUS-2020-Report.pdf

[3] National Security Council, Prime Minister's Department. (2020) Malaysia Cyber Security Strategy 2020-2024. https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

[4] Jian, Ng Jia, and Intan Farahana Binti Kamsin. "Cybersecurity Awareness Among the Youngs in Malaysia by Gamification." In *3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)*, pp. 487-494. Atlantis Press, 2021. https://doi.org/10.2991/ahis.k.210913.061

[5] Zichermann, Gabe, and Christopher Cunningham. *Gamification by design: Implementing game mechanics in web and mobile apps*. " O'Reilly Media, Inc.", 2011.

[6] Gjertsen, Eyvind Garder B., Erlend Andreas Gjære, Maria Bartnes, and Waldo Rocha Flores. "Gamification of Information Security Awareness and Training." In *ICISSP*, pp. 59-70. 2017. https://doi.org/10.5220/0006128500590070

[7] Scholefield, Sam, and Lynsay A. Shepherd. "Gamification techniques for raising cyber security awareness." In *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21*, pp. 191-203. Springer International Publishing, 2019. https://doi.org/10.48550/arXiv.1903.08454

[8] Shen, Low Wan, Hazinah Kutty Mammi, and Mazura Mat Din. "Cyber Security Awareness Game (CSAG) for Secondary School Students." In *2021 International Conference on Data Science and Its Applications (ICoDSA)*, pp. 48-53. IEEE, 2021. https://doi.org/10.1109/ICoDSA53588.2021.9617548

[9] PulseLearning. Gamification. https://www.pulselearning.com/gamification/

[10] Koziol, J. and Bottorff, C. (2022). "Cybersecurity Awareness: What It Is and How to Start", FORBES, Mar 16.

[11] Cybersecurity Annual Report (2021). https://www.cybersecurity.my/en/media_centre/annual_report/main/main/detail/1912/index.html

[12] Maalem Lahcen, Rachid Ait, Bruce Caulkins, Ram Mohapatra, and Manish Kumar. "Review and insight on the behavioral aspects of cybersecurity." *Cybersecurity* 3, no. 1 (2020): 1-18. https://doi.org/10.1186/s42400-020-00050-w

[13] Mubarak, A. R. "Child safety issues in cyberspace: A critical theory on trends and challenges in the ASEAN region." *International Journal of Computer Applications* 129, no. 1 (2015): 48-55. https://doi.org/10.5120/ijca2015906925

[14] Garba, Adamu, Maheyzah Binti Sirat, Siti Hajar, and Ibrahim Bukar Dauda. "Cyber security awareness among university students: A case study." *Science Proceedings Series* 2, no. 1 (2020): 82-86. https://doi.org/10.31580/sps.v2i1.1320

[15] Espinha Gasiba, Tiago, Ulrike Lechner, and Maria Pinto-Albuquerque. "Sifu-a cybersecurity awareness platform with challenge assessment and intelligent coach." *Cybersecurity* 3 (2020): 1-23. https://doi.org/10.1186/s42400-020-00064-4.

[16] Potgieter, Pieter. "The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology." In *ICICIS*, pp. 272-280. 2019. https://doi.org/10.29007/gprf

[17] Zahri, Y., R. Susanty, A. and Mustaffa, A. "Cyber Security Situational Awareness among Students: A Case Study in Malaysia". *World Academy of Science, Engineering and Technology International Journal of Educational and Pedagogical Sciences 11*, no. 7 (2017): 1654-1660.

[18] Malaysia Education Ministry. (November, 2020), Notice of Implementation of Teaching and Learning at Home (PDPR), https://www.moe.gov.my/en/pemberitahuan/announcement/pemakluman-pdpr

[19] Zahri, Yunos, R. Susanty Ab Hamid, and Ahmad Mustaffa. "Cyber security situational awareness among students: a case study in Malaysia." *International Journal of Educational and Pedagogical Sciences* 11, no. 7 (2017): 1704-1710. https://doi.org/10.5281/zenodo.1131053

[20] Asokhia, M. O. "Enhancing national development and growth through combating cybercrime/Internet fraud: a comparative approach." *Journal of Social Sciences* 23, no. 1 (2010): 13-19. https://doi.org/10.1080/09718923.2010.11892806

[21] Zulkifli, Zahidah, Nurul Nuha Abdul Molok, Nurul Hayani Abd Rahim, and Shuhaili Talib. "Cyber Security Awareness Among Secondary School Students in Malaysia." *Journal of Information Systems and Digital Technologies* 2, no. 2 (2020): 28-41.

[22] "DiGi CyberSAFE the National Survey Report 2015: Growing Digital Resilience among Malaysian Schoolchildren on Staying Safe Online," DiGI, CyberSecurity Malaysia, Kementeri. Pendidik. Malaysia, 2015.

[23] VTT Technical Research Centre of Finland. (2018). ASEAN Cybersecurity Innovation Ecosystem: A Co-creation approach, pp. 32-42. Retrieved from https://projectyaksha.eu/wp-content/uploads/2019/05/D1.2_ASEAN-Cybersecurity-Ecosystem-a-cocreation-approach_vf.pdf

[24] Larose, Daniel T. *Discovering statistics*. Macmillan Higher Education, 2015.

[25] Walpole, R.E., Myers, R.H., Myers, S.L and Ye K.E. (2011). Probability and Statistics for Engineers and Scientists (9th Edition) 9th edition, Pearson.