Available online at
https://jcrinn.com/
https://crinn.conferencehunter.com/

Journal of Computing Research and Innovation 10(1) 2025

Journal of Computing Research and Innovation

Cyber Security Awareness on Social Media: Knowledge Sharing Among Orang Asli Students

Palaniappan Shamala[1*], Muruga Chinniah[2], Shamsatun Nahar Binti Ahmad[3], Lee Chang Kerk[4], Abd Malik Bin Mohd Rick[5]

[1,3,4,5]College of Computing, Informatics, and Mathematics, Universiti Teknologi MARA (UiTM) Johor Branch, Segamat Campus, 85000 Johor, Malaysia
[2]Faculty of Business Management, Universiti Teknologi MARA (UiTM) Johor Branch, Segamat Campus, 85000 Johor, Malaysia

ARTICLE INFO

Article history:
Received 24 October 2024
Revised 31 December 2024
Accepted 11 January 2025
Online first
Published 1 March 2025

Keywords:
Cybersecurity
Awareness
Privacy setting
Social Media
Orang Asli
Peer-to-peer

DOI:
10.24191/jcrinn.v10i2

ABSTRACT

Cybersecurity is becoming more vital as we rely on digital devices and technology to navigate our everyday lives. When access to cyberspace is unrestricted to all levels of age, children use the internet daily for purposes like playing online games, using social media, or even doing their schoolwork. These circumstances have created an environment that makes them vulnerable to cybercrime threats. Therefore, the need to create awareness and training on cybersecurity is vital. However, our awareness program on safety protocol, and information privacy settings in WhatsApp, TikTok, and Instagram was aimed at Orang Asli students because they reside in rural regions with increasing access to digital technologies. Thus, targeted cybersecurity education can help them bridge the knowledge gap and protect them from online risks. The methodology consists of four phases: Phase 1: MCMC as the governmental body runs awareness campaigns, Phase 2 & 3: secondary students from SMK Bekok undergo expert-led training and workshops from lecturers, and Phase 4: create a sustainable educational cycle, wherein secondary students transmit their knowledge to primary students. In each phase, sets of questionnaires with pre and post-tests were distributed to assess the program's impact. The results showed the program has successfully achieved its objectives of enhancing cybersecurity awareness among Orang Asli students. Knowledge transfer by applying a peer-to-peer approach gained better comprehension, higher engagement, and more effective learning outcomes. In addition, cultivates a collaborative learning atmosphere that advantages both students, simultaneously enriching the educational experience and fostering community engagement within the school.

1. INTRODUCTION

Cybersecurity is a measurement for protecting computer systems, networks, and information. It helps to prevent our digital landscape from disruption or unauthorized access, use, disclosure, modification, or

[1*] Corresponding author. *E-mail address*: shamalap@uitm.edu.my
https://doi.org/10.24191/jcrinn.v10i1.495

destruction (Florackis et al., 2023). Therefore, to ensure online safety for every Internet user, delivering cybersecurity awareness among our community is essential and cannot be neglected. Technology has become an integral part of our daily life, almost everyone has access to cyberspace. It has changed our lifestyle, especially during and after the COVID-19 pandemic, it influences activities like connecting with friends, running businesses, doing shopping, and so on (Aphane, 2023). However, the increasing use of cyberspace has also made citizens vulnerable to cybercrime threats (Ciso, 2024). Based on the research, the penetration of the Internet for Malaysians has increased over the decades, along with it, the cybersecurity issue has also been on the rise (Ganesin et al. 2016; Pawar & Palivela, 2022).

In Malaysia, there are a lot of ethnic groups. Orang Asli is one of them. Among others, this community needs more attention, because the Orang Asli population exists in a state of segregation and seclusion from the predominant trajectory of national progress (Harun & Hamid, 2010). This group is characterized by distinct linguistic, cultural, lifestyle, and physical attributes. In comparison to other ethnic communities, the Orang Asli demographic continues to fall behind in numerous domains (Kamsim, 2021). Consequently, they frequently encounter significant barriers to accessing fundamental resources, such as education and technology, thereby rendering them particularly susceptible to the evolving threats posed by cybersecurity.

Some youth Orang Asli have stepped into the city to pursue higher education, but many of them still live in the rural areas (Ooi, 2007; Huey & Ferguson, 2022). There are also a lot of attempts have been made to build up the bridge between Orang Asli and the digital world, such as the advocacy and outreach programme in Sembilan state. This program focuses the young generation within the Orang Asli community to promote best practices in internet usage (Bernama, 2024).

Recently, Internet scams are on the rise, and it's not just clueless folks getting caught; teachers are falling for them too. Take the case from 2019, when an Orang Asli teacher lost RM3680 to a scam (Tahir, 2019). This not only put a dent in her wallet but also made her seriously question her knowledge about cybersecurity. Fast forward to 2024, another teacher getting scammed for a whopping RM135,150 (Awang, 2024). These incidents really show how crucial it is to educate people about cybersecurity, especially in remote areas. So, it’s a good idea for educational programs in the communities to cover the basics of cybersecurity to help the people spot and avoid potential online threats.

In order to ensure the safety of our digital environment, create awareness among citizens is a must. The Orang Asli community also cannot be excluded. A robust education in cybersecurity will be increasingly vital for enhancing our quality of life in the future and equipping us with the tools to mitigate potential threats. Therefore, the objectives of this research are to increase information security and privacy awareness among the teenagers of Orang Asli and to provide effective education on setting up social media applications safely and privately. To achieve the targets, a series of activities have been conducted in collaboration with SMK Bekok and SK Kampong Kudong in Segamat.

Through these activities, the selected secondary students who are majority formed by the young generation of Orang Asli will learn about the importance of cybersecurity and how to protect themselves online, thereby helping them avoid becoming victims of cyber-attacks. Then, the transfer knowledge session will be carried out. Those secondary students will be the facilitators to transmit the input to primary school students at SK Kampong Kudong. The details will be discussed in the next section.

2. RELATED WORK

In the field of social media and its impact on various aspects of society, many studies have been conducted to understand the dynamics of online platforms. Shaw et al. (2015) emphasize a rigorous methodological process and delve deep into how adolescents interact with social media, shedding further light on the use of social media as an adolescent health intervention. This highlights the need to investigate how young people interact with such online platforms and how it impacts their well-being.

https://doi.org/10.24191/jcrinn.v10i1.495

Furthermore, Goodyear and Armour (2018) use empirical case studies and evidence from various stakeholders to explore the opportunities and risks associated with social media use. Clearly, these highlight the complexity of digital space and the range of different impacts it can have on individuals, including young people.

2.1 Young people's Use of Social Media

Social media use by young people is an interesting topic for researchers. Wang and Edwards (2016) argue that what adults perceive as cyberbullying may be considered normal behaviour for young people, suggesting different understandings of online interactions among different age groups. This highlights the need to bridge the perception gap and understand the nuances of young users' online behaviour. Furthermore, Décieux et al. (2018) conducted a mixed-methods study to investigate the role of social media in promoting friendship-focused interactions among young people. Her research provides insight into how online platforms foster and shape social relationships among young people and highlights the need to understand the dynamics of virtual connections in today's society.

2.2 Threats on Social Media

When considering the threats posed by social media platforms, issues such as identity theft, phishing, and cyberbullying emerge as major concerns. Albulayhi and Khediri (2022) conducted a comprehensive study on privacy and security issues in social networks, highlighting the various threats and privacy issues that users may encounter. Understanding these challenges is important to develop effective strategies to mitigate risks and increase users' cybersecurity awareness. Furthermore, Webb et al. (2022) questioned whether social media use contributes to increased rates of intentional self-harm and suicide among Australian youth. This highlights how online interactions can have a negative impact on mental health and underlines the need to address the harmful effects and promote safe online behaviour among young people.

2.3 Reasons behind Social Media Security Issues

The underlying reasons for security issues in social media platforms are manifold. Authentication, security and privacy concerns, and the prevalence of fake profiles are among the major factors that exacerbate security vulnerabilities. Agarkar and Agrawal (2019) highlighted the importance of authentication and privacy systems in addressing cybersecurity issues and emphasized the crucial role of robust security measures in protecting online interactions. Furthermore, Nithya and Rekha (2023) discussed the adoption of biometric authentication in social media security, with a particular focus on iris recognition to improve the authentication process. Their findings highlight the evolving nature of security measures in online platforms and the need for innovative approaches to effectively counter emerging threats.

2.4 Security Awareness Program Methods

Table 1 shows that implementing various methodologies to instill security awareness among students in academic institutions is essential for cultivating a safe and secure environment. Diverse strategies, including interactive workshops, gamification, trainer training, instructor-led instruction, the involvement of external experts, and the utilization of engaging multimedia content, can accommodate various learning modalities and demographic age ranges.

https://doi.org/10.24191/jcrinn.v10i1.495

Table 1. Summary of methods apply in cybersecurity awareness program

Author/ year	Summary of Paper			
	Delivery Method Applied	**Content Covered**	**Participate**	**Platform**
Alotibi (2024)	Security Training Programs, Comprehensive Security Policies, Awareness Campaigns, Engaging External Experts, Parent Involvement, & Technology Integration	Privacy settings, cybersecurity best practices, risk awareness, and responsible digital citizenship	Saudi school children	Social media
Jalil et al. (2024)	(i) Training of Trainers' course offered by Cybersecurity Malaysia (ii) Development of training modules (iii) A cybersecurity awareness program was conducted online using the Cisco Webex application.	Introduction to Cyber Security, Cyber Security Threats and Risks, Cyber Bullying, Identity Theft, Internet Addiction, Malware, and Internet Usage Ethics.	Secondary School Students	Social media
Yeboah et al. (2024)	Instructor-led delivery technique outperformed the game-based strategy in terms of boosting users' cybersecurity awareness.	-	All level participant	Cyber world
Jian and Kamsin (2021)	Method applied: BEWARE, the cybersecurity game.	Given scenarios that had happened in real life and how to react to these threats in real-world	Teenagers	Cyber world
Molok et al. (2023)	Method applied: Digital storytelling application, called SMARTCTZEN (multimedia application that uses interactive elements to tell stories)	Strategies to recognize cyber threats, respond to these threats appropriately, and make informed decisions about their cyber behaviour.	University students in Malaysia	Cyber world

These methodologies serve to educate students regarding potential risks and safety protocols. In addition, it also empowers them to make informed choices, identify threats, and respond appropriately. By integrating a multifaceted technique, educational institutions can develop a comprehensive and effective security awareness initiative. This technique may equip students with the requisite knowledge and skills to safely navigate both physical and digital environments.

3. METHODOLOGY

The project involves the development of a cybersecurity awareness module that will help raise the level of security awareness in using social media among Orang Asli primary and secondary school students. The main attributes of our module that distinguish it from other available cybersecurity awareness modules are our method aiming to gain a sustainable educational and support framework within the school community. The goals are to foster lasting security awareness using social media and knowledge transfer by applying a peer-to-peer approach for better comprehension, higher engagement, and more effective learning outcomes.

Peer-to-peer teaching enhances knowledge retention, builds confidence, and improves comprehension for both tutors and learners. Research supports that when students teach their peers, consolidates understanding, fosters collaboration, and leads to higher academic achievement and self-efficacy. This approach also encourages active engagement, responsibility for learning, and the development of communication and leadership skills (Johnson & Johnson, 2020).

In this cybersecurity awareness program, two key tasks have been implemented: planning and implementation. Planning is integral to the successful implementation of a cybersecurity awareness program. It provides a structured framework that bridges the gap between strategic objectives and actionable steps. Outlining what to teach, how to teach, and who should teach may ensure that the implementation phase proceeds in a systematic and coordinated manner.

https://doi.org/10.24191/jcrinn.v10i1.495

3.1 Planning

The planning for this awareness program was based on the results demonstrated by Boulton et al. (2016). The themes delineated in the systematic literature review by Boulton et al. (2016) on cyber security education for children were what to teach, how to teach, and who should teach. By exploring these questions, researchers can ensure the implementation of comprehensive and effective cybersecurity education programs.

3.1.1 What to teach

The awareness program focuses on three key areas: (a) identifying the types of threats and dangers users may encounter, (b) understanding and implementing safety protocols, and (c) managing information privacy settings on popular social media platforms such as WhatsApp, TikTok, and Instagram. Table 2 shows the reason for choosing these three most vulnerable social platforms.

Table 2. Social platforms and reasons

Social media	Reason
WhatsApp	Malaysian Communications and Multimedia Commission (MCMC) Internet Users Survey 2022: WhatsApp is the most used social platform by students for instant messaging, voice and video calls, and sharing multimedia content like photos, videos, and documents.
TikTok	According to the MCMC Internet Users Survey 2022, TikTok is one of the fastest-growing platforms among young users in Malaysia for entertainment, with students often spending significant time on the app.
Instagram	Statista provides data on Instagram's user demographics and engagement. As of 2023, Instagram boasts over 1 billion global monthly active users, which comprises teenagers and young adults.

3.1.2 How to teach & Who should teach

This program aims to cultivate a collaborative learning atmosphere that advantages both students, simultaneously enriching the educational experience and fostering community engagement within the school. Cybersecurity education involves a diverse range of stakeholders, primarily categorized into three groups (Zulkifli et al., 2023) (a) governmental bodies, (b) school/teachers and (c) parents. Each group plays a crucial role in fostering a secure and informed digital environment. By carefully planning what to teach, who to teach, and how to teach, it was ensured the program was successfully organized and met its educational objectives, as shown in Fig. 1.

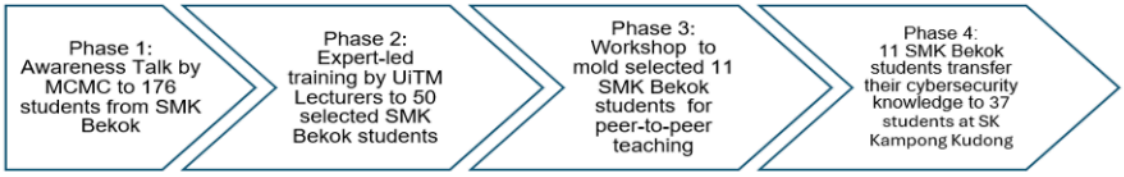

Fig. 1. Flow of four main phases

This awareness program was planned to be carried out in four main phases. In phase 1, MCMC as a governmental body is chosen to give cybersecurity awareness education as they possess the authority to set national standards and ensure widespread adherence to security protocols. According to Johnson and Madnick (2021), governmental bodies also ensure access to up-to-date resources and collaboration with industry experts to address evolving cyber threats.

In phases 2 and 3, expert-led training and workshops were chosen for students to gain a deep understanding of cybersecurity from lecturers who have practical experience in the cybersecurity field. Trained students will pass on their knowledge to younger students through peer-to-peer teaching. This stage

https://doi.org/10.24191/jcrinn.v10i1.495

emphasizes building knowledge acquisition, comprehension, and self-assurance (Smith 2023). This approach fosters a sustainable learning environment. Students trained by experts will mentor primary students, reinforcing the concepts and expanding the reach of cybersecurity education (Smith & Brown, 2020). In addition, the peer awareness method, also agreed upon by Ayyash et al. (2024), proved that students were more receptive and had a better comprehension of the information and training when they received it from the older students than any other method (Sağlam et al., 2023).

Phase 4 trained secondary students of SMK Bekok transfer the cybersecurity knowledge to primary students at SK Kampong Kudong. In each phase, a set of questionnaires with pre- and post-tests was distributed to assess the impact of the program.

3.2 Implementation

The implementation section outlines when each phase of the cybersecurity awareness program was executed and who was responsible for carrying it out. Detailed outcomes and findings from each phase are presented in the results section. Table 3 explains activities carried out in each phase.

Table 3. Activities carried out in each phase

Phase	Activity
Phase 1	On 25 June 2023, MCMC as the governmental body, was invited to run awareness campaigns to enhance students's understanding of digital safety, encompassing secure online behaviors, identification of cyber threats, and safeguarding personal data. MCMC conducted a seminar titled "Awareness of Cybersecurity & Information Security" for 176 secondary students at SMK Bekok.
Phase 2	On 18 July 2023, out of 176 students, only 50 secondary students from SMK Bekok were selected to undergo expert-led training from lecturers from the Universiti Teknologi Mara Johor Branch (UiTMJ).
Phase 3	On 1 August 2023, out of 50 students, only eleven students were selected for appointments as facilitators for peer-to-peer teaching, who then transferred their knowledge about information security to primary school students. This phase ensures facilitators are well-prepared to deliver the awareness message effectively.
Phase 4	On 24 September 2023, SMK Bekok Secondary students effectively imparted information security knowledge to Orang Asli children at SK Kampong Kudong. This approach can create a sustainable educational cycle.

4. RESULTS AND DISCUSSION

This research used a non-probability sampling method based on student availability, as commonly done in community service studies where random selection is not feasible (Tashakkori & Teddlie, 2021). Thus, this research use of available participants was deemed appropriate, reflecting common fieldwork constraints. Results of the study are presented in the following phases:

4.1 Phase 1: Selection of Students

Students were given a set of quiz questions containing five multiple-choice questions and 10 true or false questions after the Malaysian Communications Multimedia Commission (MCMC) talk. The quiz is given to measure the number of students who have a high level of understanding of the speaker's presentation on cyber security and information security. A total of 176 students from SMK Bekok, which are breakdown to Form 1 (19.9%), Form 2 (14.2%), Form 3 (26.70%), and Form 4 (39.50%), have participated in the MCMC talk. The students' quiz scores between 11 and 15 were used to screen them for entry into the second phase. Given that the maximum quiz score is 15, we deemed scores of 70% and higher as appropriate for selection (Smith & Lee, 2021). Students are evaluated not only through quizzes but also based on their active participation during the lecture, including asking and answering questions and sharing their opinions. Each active contribution is acknowledged with a sticker. As a result, a sample of 50 students from Form 1 to Form 4 (30 females and 20 males) met the selection criteria. These criteria reflect a higher level of engagement and understanding of data privacy issues. It was challenging to choose samples for this

https://doi.org/10.24191/jcrinn.v10i1.495

study because it was difficult to engage with Orang Asli students due to their naturally shy and humble attitude.

4.2 Phase 2: Analysis of the Awareness of Students

A cybersecurity and information security on social media workshop was conducted to enlighten awareness among the school students. A 5-point Likert-scale questionnaire was given to 50 students before and after the workshop. The questionnaire consists of 10 items. The results are summarized in Table 4.

Table 4. Summary of Data Collection for Phase 2

Question	Mean		Mean Difference	Variance		Pearson Correlation	t-Stat	t-Critical two-tail
	Pre	Post		Pre	Post			
Q1	2.6	3.94	1.34	0.3673	0.4249	0.1963	-11.8706	±2.0096
Q2	2.86	4.18	1.32	0.8167	0.3955	0.2248	-9.5425	±2.0096
Q3	2.38	3.92	1.54	0.7302	0.4016	0.3211	-12.2977	±2.0096
Q4	2.08	3.72	1.64	0.8506	0.5322	0.1553	-10.7033	±2.0096
Q5	2.18	3.70	1.52	0.9669	0.9490	-0.0064	-7.7403	±2.0096
Q6	2.84	4.30	1.46	0.9127	0.5408	0.3021	-10.1773	±2.0096
Q7	2.76	4.04	1.28	0.5943	0.7331	0.1385	-8.4604	±2.0096
Q8	2.42	3.98	1.56	0.6159	0.5506	0.1199	-10.8852	±2.0096
Q9	2.86	4.04	1.18	0.7351	0.4882	0.3502	-9.3074	±2.0096
Q10	2.52	4.00	1.48	0.7853	0.5714	0.3960	-11.5140	±2.0096

Detail analysis presented in this paper is for each question.

(i) Question 1: Understanding Types of Threats in Online Applications

The analysis shows a mean difference of 1.34, indicating a significant increase in participants' perceptions of their understanding regarding online threats. Variance slightly increase from 0.3673 to 0.4249, suggesting more varied opinions post-intervention. The Pearson correlation coefficient of 0.1963 indicates a weak positive relationship, suggesting that those with higher initial understanding tended to maintain that view, though the correlation is weak.

(ii) Question 2: Social Media and Data Awareness

The mean difference of 1.32 highlights a substantial increase in awareness regarding data collection by social media. Variances decreased from 0.8167 before the intervention to 0.3955 afterward, suggesting that participants' perceptions became more consistent. The Pearson correlation coefficient of 0.2248 reveals a weak positive relationship, indicating those with higher awareness before the workshop tended to maintain that awareness afterward.

(iii) Question 3: Knowledge of Information Security

The mean difference of 1.54 indicates a significant increase in participants' knowledge of information security. Variance decrease from 0.7302 to 0.4016, indicating a more consistent understanding. The Pearson correlation coefficient of 0.3211 indicates a moderate positive correlation, suggesting that participants with some prior knowledge tended to improve their understanding post-intervention, although outliers exist. Overall, these findings reflect a robust positive outcome from the intervention.

(iv) Question 4: Knowledge of Data Phishing

The analysis demonstrates that the intervention effectively enhanced participants' knowledge regarding data phishing techniques, as evidenced by a mean difference of 1.64. The reduction in variance post-intervention suggests a more uniform understanding among participants. Although the correlation is weak,

https://doi.org/10.24191/jcrinn.v10i1.495

the significant t-statistic indicates a strong overall positive effect of the educational initiatives concerning data phishing.

(v) Question 5: Ability to Share Knowledge about Online Safety

The intervention significantly boosted participants' confidence in sharing online safety knowledge, with mean difference of 1.52. Although variances were similar and the Pearson correlation was weak (-0.0064), the t-statistic confirms a substantial positive shift in participants' attitudes toward sharing this knowledge.

(vi) Question 6: Knowledge of Creating Strong and Secure Passwords

The intervention effectively improved participants' knowledge of creating secure passwords, with mean difference of 1.46. A reduction in variance post-intervention indicates a more consistent understanding, while a moderate Pearson correlation supports the positive impact of the educational efforts.

(vii) Question 7: Knowledge of Using Social Media Safely

The intervention significantly improving participants' understanding of safe social media practices, with a mean difference of 1.28. The increased variance post-intervention indicates varied knowledge gains among participants. A weak Pearson correlation suggests a slight relationship between pre-existing knowledge and post-intervention outcomes, highlighting the effectiveness of the educational efforts.

(viii) Question 8: Knowledge of Handling Issues with Online Purchases

The intervention significantly improved participants' understanding of appropriate responses to problems encountered during online purchases, with a mean difference of 1.56. The decrease in variance post-intervention reflects a more uniform comprehension. The very weak Pearson correlation suggests a limited influence of prior knowledge. Overall, the results reflect a positive outcome from the educational initiative.

(ix) Question 9: Knowledge of Safe Usage of Online Applications

The intervention significantly enhancing participants' understanding of safe practices for using online applications, with a mean difference of 1.18. The decrease in variance indicates more consistent understanding. The moderate Pearson correlation suggests the prior knowledge influenced post-intervention results, reinforcing the effectiveness of the educational efforts.

(x) Question 10: Knowledge of Making Safe Online Purchases

The intervention significantly improved participants' knowledge of safe online purchases, with a mean difference of 1.48. The reduction in variance shows more consistent understanding, and the moderate Pearson correlation indicates a relationship between prior knowledge and post-intervention comprehension, highlighting the success of the educational initiative.

4.3 Phase 3: Selection of Facilitators

Based on the results from Phase 2, eleven students were selected for appointments as facilitators, who then transferred their knowledge about information security to primary school students. The criteria for selection are the highest mean between 4 and 5. These students went through the training workshop and were able to answer all questions from the given module.

4.4 Phase 4: Analysis from Transfer Knowledge

A survey of 37 students at SK Kampong Kudong was conducted to test their understanding of information security, which is divided into risk (four items) and security protocol (five items). They were asked to

https://doi.org/10.24191/jcrinn.v10i1.495

answer either "yes" or "no" for each item. Table 5 presents the data. Table 5 shows a significant increase in cybersecurity awareness across all questions after the intervention. The difference in percentage before and after the workshop shows a positive value. This proves a positive, progressive development of understanding of risk and security protocols on social media applications among 37 primary students. This means that social media applications are common among primary students these days. In addition, peer-to-peer method is the effective way to transfer knowledge.

Table 5. Summary Data Collection for Phase 4

Knowledge about cybersecurity	Mean Answer "yes" in percent (%)		Mean Difference
	Before	After	
Risk (4 questions)	41.22	81.08	39.86
Security protocol (5 questions)	26.49	84.87	58.38

5. CONCLUSION AND RECOMMENDATION

Raising cybersecurity awareness is crucial for empowering marginalized communities like the Orang Asli, who may lack knowledge and protection against online threats. In this study, students from SMK Bekok, where the majority are Orang Asli, were selected as facilitators to deliver cybersecurity content to primary students at SK Kampong Kudong, also predominantly Orang Asli. The knowledge transfer was successful, as evidenced by the positive impact on the students' cognitive understanding of cybersecurity, significantly enhancing their knowledge and awareness. This contributes to creating a safer online environment for everyone. This study not only benefits the Orang Asli community by improving their digital literacy and safeguarding their online activities, but it also demonstrates the effectiveness of implementing cybersecurity awareness among the youths of Orang Asli. Moreover, the success of this initiative highlights the potential for scaling similar programs to other marginalized communities, fostering a culture of cybersecurity from a young age. By empowering these communities with the knowledge and tools to protect themselves online, we can contribute to a more secure and inclusive digital landscape, ultimately reducing the digital divide and ensuring that no one is left vulnerable to cyber threats. To improve current efforts, it would be helpful to include teachers and parents in future to enhance cybersecurity education at home and in schools, creating a better learning environment. Additionally, looking into digital tools and game-based learning will also increase engagement and understanding, particularly for younger learners, which would contribute to a friendlier and safer online community.

6. ACKNOWLEDGMENTS

The research is supported by CE-SIR2023 grant, with project code: 600-RMC/CE-SIR 5/3 (017/2023), Industry Community and Alumni Network (ICAN), Community Network Centre (CNC) and registered with Research Management Centre (RMC), UiTM.

7. CONFLICT OF INTEREST STATEMENT

The authors agree that this research was conducted in the absence of any self-benefits, commercial or financial conflicts and declare the absence of conflicting interests with the funders.

8. AUTHORS' CONTRIBUTIONS

All authors are involved in the whole process of this research.

https://doi.org/10.24191/jcrinn.v10i1.495

9. REFERENCES

Aphane, M. P. (2023). Cybersecurity awareness on cybercrime among the youth in Gauteng Province. *International Journal of Social Science Research and Review*, *6*(8), 23-32.

Agarkar, A., & Agrawal, H. (2019). A review and vision on authentication and privacy preservation schemes in smart grid network. *Security and Privacy*, 2(2), e62. https://doi.org/10.1002/spy2.62

Alotaibi, G. (2024). A cybersecurity awareness model for the protection of saudi students from social media attacks. *Engineering, Technology & Applied Science Research*, *14*(2), 13787-13795. https://doi.org/10.48084/etasr.7123

Ayyash, M., Alsboui, T., Alshaikh, O., Inuwa-Dute, I., Khan, S., & Parkinson, S. (2024). Cybersecurity education and awareness among parents and teachers: A survey of Bahrain. *IEEE Access*, *12*, 86596-86617. https://doi.org/10.1109/ACCESS.2024.3416045

Albulayhi, M. S., & El Khediri, S. (2022). A comprehensive study on privacy and security on social media. *International Journal of Interactive Mobile Technologies*, *16*(1), 1-18.

Awang, A (2014). Guru wanita rugi RM135,150 angkara phone scam. https://www.bharian.com.my/berita/kes/2024/07/1273869/guru-wanita-rugi-rm135150-angkara-phone-scam

Boulton, M. J., Boulton, L., Camerone, E., Down, J., Hughes, J., Kirkbride, C., ... & Sanders, J. (2016). Enhancing primary school children's knowledge of online safety and risks with the CATZ Cooperative Cross-Age Teaching Intervention: Results from a pilot study. *Cyberpsychology, Behavior, and Social Networking*, *19*(10), 609-614. https://doi.org/10.1089/cyber.2016.004

Bernama. Negeri Sembilan orang asli advocacy and outreach programme wins WSIS 2024 Award. https://www.bernama.com/en/news.php?id=2289356. 2019.

Ciso, (2024) JIL Information Technology. Cybersecurity Awareness Hand Book,chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.jiit.ac.in/sites/default/files/Cyber%20Security%20Awareness%20Hand%20Book.pdf.

Décieux, J. P., Heinen, A., & Willems, H. (2019). Social media and its role in friendship-driven interactions among young people: A mixed methods study. *Young*, *27*(1), 18-31. https://doi.org/10.1177/1103308818755516

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies*, *36*(1), 351-407. https://doi.org/10.1093/rfs/hhac024

Ganesin, A., Supayah, L., & Ibrahim, J. (2016). An overview of cyber security in Malaysia. *Arabian Journal of Business and Management Review (Kuwait Chapter)*, *6*(4), 12-20. https://j.arabianjbmr.com/index.php/kcajbmr/article/view/956

Goodyear, V. A., & Armour, K. M. (2019). *Young people, social media and health* (p. 232). Taylor & Francis.

Huey, L., & Ferguson, L. (2022). *Another digital divide: Cybersecurity in Indigenous communities*.
https://doi.org/10.24191/jcrinn.v10i1.495

CrimRxiv.

Jalil, M., Ali, N. H., Yunus, F., Zaki, F. A. M., Hsiung, L. H., & Almaayah, M. A. (2024). Cybersecurity awareness among secondary school students Post Covid-19 pandemic. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 37(1), 115-127.

Jian, N. J., & Kamsin, I. F. B. (2021, September). 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. https://doi.org/10.2991/ahis.k.210913.061

Johnson, S., & Madnick, S. (2021). Government's role in shaping cybersecurity education: Policies and frameworks for national security. *Cybersecurity Journal*, *15*(2), 78-92.

Johnson, D. W., & Johnson, R. T. (2020). *Cooperation and competition: Theory and research*. Interaction Book Company.

Kamsin, I. F., Khalid, F., Salleh, N. S. M., Hamdan, A., & Manaf, S. Z. A. (2021). The impact of orang asli students' learning styles on their achievement of meaningful learning. *International Journal of Engineering and Advanced Technology*, *9*(6), 285-292.

Nithya, S., & Rekha, B. (2023). Insights on data security schemes and authentication adopted in safeguarding social network. *International Journal of Advanced Computer Science and Applications*, *14*(4), 474-483. https://www.proquest.com/openview/d7fd995deffc169ff9f9298ef89c0cb9/1?pq-origsite=gscholar&cbl=5444811

Noraida Harun & Noor Ashikin Hamid (2010). Akta Orang Asli 1954 (Akta 134): Sejauh mana melindungi hak orang asli: Satu kajian perbandingan. https://www.unisza.edu.my/perpustakaan/images/IDC/orang%20asli.pdf

Molok, N. N. A., Sapee, N., & Othman, A. A. (2023). Smart Ctzen: A digital storytelling app to empower youth's awareness in cyber safety and security. *Journal of Information Systems and Digital Technologies*, *5*(2), 108-120. https://doi.org/10.31436/jisdt.v5i2.436

Ooi, P. H. Y. (2007). ICT and the Orang Asli in Malaysia. In L. E., Dyson (Ed.), *Information technology and indigenous people* (pp. 55-57). IGI Global. https://doi.org/10.4018/978-1-59904-298-5.ch006

Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, *2*(1), 100080. https://doi.org/10.1016/j.jjimei.2022.100080

Sağlam, R. B., Miller, V., & Franqueira, V. N. (2023). A systematic literature review on cyber security education for children. *IEEE Transactions on Education*, *66*(3), 274-286. https://doi.org/10.1109/TE.2022.3231019

Smith, J.J., (2023). *Educators' perspectives on cybersecurity educational resources* [Doctoral dissertation, Carleton University].

Smith, J., & Brown, L. (2020). The impact of expert-led cybersecurity education on student readiness. *Journal of Information Security*, *12*(3), 45-60.

Smith, J., & Lee, K. (2021). Establishing effective academic progression criteria: A study on selection thresholds for intervention programs. *Journal of Educational Assessment*, *45*(2), 123-137. https://doi.org/10.1016/j.jedut.2020.12.003

Shaw, J. M., Mitchell, C. A., Welch, A. J., & Williamson, M. J. (2015). Social media used as a health

intervention in adolescent health: A systematic review of the literature. *Digital Health*, 1, 2055207615588395. https://doi.org/10.1177/20552076155883

Tashakkori, A., & Teddlie, C. (2021). *Mixed Methodology: Combining Qualitative and Quantitative Approaches* (3rd ed.). Sage.

Tahir (2019) Guru Orang Asli rugi ditipu scammer. https://www.sinarharian.com.my/article/47234/edisi/pahang/guru-orang-asli-rugi-ditipu-scammer

Wang, V., & Edwards, S. (2016). Strangers are friends I haven't met yet: a positive approach to young people's use of social media. *Journal of Youth Studies*, *19*(9), 1204-1219. https://doi.org/10.1080/13676261.2016.1154933

Webb, B., Looi, J. C., Allison, S., Bidargaddi, N., & Bastiampillai, T. (2022). Point of view: Could social media use be contributing to rising rates of deliberate self-harm and suicide in Australian youth populations?. *Australasian psychiatry*, *30*(6), 694-697. https://doi.org/10.1177/10398562221100093

Yeboah, A.D. and Gyebi, E.B., (2024). Comparison between gamification and instructor-led as user methods for effective cyber security awareness delivery. *International Journal of Information Technology and Language Studies*, *8*(1).

Zulkifli, N., Ahmad, S.R., Yusoff, W.Y.W., Ahmad, A. and Amran, M.F.M., 2023. MCMC (DFRMS-MCMC). APS, p.371.

https://doi.org/10.24191/jcrinn.v10i1.495