International Journal of Advanced Research in Education and Society
e-ISSN: 2682-8138 | Vol. 7, No. 3, 384-390, 2025
https://asianscholarsnetwork.com/asnet-journals

Awareness of Cyber Fraud and Public Knowledge Among Undergraduate Students

Ismariani Ismail[1*], Adeline Engkamat[1], Lee Yee Ann[1], Azlina Bujang[1], Zubaidah Bohari[1]

[1] Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Sarawak, Malaysia

*Corresponding Author: ismariani@uitm.edu.my

Received: 30 April 2025 | Accepted: 2 June 2025 | Published: 30 June 2025

DOI: https://doi.org/10.55057/ijares.2025.7.3.34

Abstract: *Cyber fraud is a growing problem in Malaysia, with a significant increase in the number of cases and losses in recent years. The majority of those who fell victim to cyberattacks chose not to escalate the matter, did not report these crimes to the authorities or did not take any further actions to protect themselves. Therefore, this study aimed to measure the awareness of cyber fraud and public knowledge among undergraduate students in UiTM Sarawak, Malaysia. In this study, online surveys were conducted and were used for data collection. A total of 171 respondents have been involved in this survey. Data were analysed using descriptive statistics. The analysis showed that respondents had low level of knowledge about Phishing scams (Mean = 2.59) and had medium level of knowledge about Macau scams (Mean = 2.71). For awareness in cyber fraud, respondents had greater awareness of Macau scams compared to Phishing scams. Thus, more awareness on cyber fraud among Malaysian students is still needed and more targeted educational initiatives and enhanced anti-fraud publicity strategies and policy development to combat cyber fraud effectively.*

Keywords: cyber fraud, public knowledge, cybercrime, awareness, undergraduate students

1. Introduction

Cyber fraud is an increasingly significant threat in the digital age, where various forms of fraud such as identity theft, phishing attacks, and financial fraud often target unsuspecting Internet users. In the context of undergraduate students, this group is frequently exposed to the risk of cyber fraud due to their extensive use of technology in their daily lives, including for learning, entertainment, and communication. However, their awareness and perception of this risk varies, depending on factors such as exposure to cyber security information, digital literacy skills, and personal experience with cyber incidents. This study focuses on the perception and awareness of undergraduate students at Universiti Teknologi MARA (UiTM) Sarawak regarding cyber fraud, to understand the extent to which this group is aware of the threat and the preventive measures taken.

Fraud cases in Malaysia are becoming increasingly alarming with 5,181 cyber security incidents recorded from January to October 2024, including 3,483 cases of online fraud (Astro Awani, 2024). Malaysia also recorded 19.62 million web attacks in the first half of 2024, thus becoming the most affected country in Southeast Asia (Dewan Kosmik, 2025). In the same

period, losses due to cybercrime reached RM1.78 billion, equivalent to over RM6 million per day (Majlis Keselamatan Negara, 2024).

With the increase in cyber fraud cases in Malaysia, this study has become increasingly relevant to evaluate the effectiveness of cyber security education and advocacy efforts among the younger generation, especially in higher education institutions. UiTM Sarawak was chosen as the study location because of the diverse student backgrounds that represent the pattern of technology use among the younger generation in Malaysia. This study also aims to identify gaps in student's knowledge and attitudes towards cyber security issues, which can be used as a basis for designing more effective educational strategies and interventions to protect them from the threat of cyber fraud.

2. Literature Review

Several studies had been conducted to gauge the awareness of cyber security and cyber fraud on different demographics. The findings from these studies vary depending on the different demographics being studied. In a study conducted among 171 undergraduate students at Afe Babalola University, Nigeria, more than half reported low levels of cybercrime consciousness (Awodiran, et al., 2023); whereas another study at Kwara State, Nigeria indicated above average level of awareness among the survey participants regarding cyber incident reporting and response (Oyelakin, 2024). From a survey regarding cyber security awareness and practices involving 253 students from Hashemite University in Jordan, it found that majority of the respondents are aware about cyber security and practices safe computer usage over the Internet (Aljammal, et al., 2024). In a more detailed study, Du and Chintakovid (2023) found that less than half of the 384 respondents from Yunnan University of Finance and Economics, China learnt about cyber security from formal courses at the university, while half of the respondents learnt from informal sources. The respondents with informal learning obtained lower scores in terms of cyber security awareness and knowledge.

Awareness of cyber security and cyber fraud can also be linked to an individual's behaviour when they faced potential cyber threats. In an interview conducted with 35 informants in four (4) cities in Malaysia, most of the informants were able to identify phishing emails and subsequently deleted it. However, several informants admitted that they prefer to make online purchases on social media instead of official sites or official accounts of the product, despite knowing that there are risks of cyber fraud when not making online purchases on regulated platforms (Pitchan, et al., 2019). Ting, et. al. (2024) distributed an online questionnaire to Malaysians of 15-30 years of age via social media sites to study the role of gender on cyber security behaviour among adolescents in Malaysia. The questionnaire focused on the respondents' behaviour towards malware, password usage, phishing, social engineering and online scam threats. A total of 207 responses had been recorded and analysed. The analysis indicated that female respondents show safer cyber security behaviour against online scams than male respondents. However, there is no significant difference found between male and female respondents' behaviour when faced with malware, password usage, phishing and social engineering.

A total of 97 individuals participated in a study focused on the susceptibility of Malaysian adults working in the banking sector towards phishing attacks. Following a thorough analysis of the survey responses, it found that cyber security awareness and culture have a positive impact on the susceptibility to phishing attacks, whereby better awareness and adoption of safe

online behaviours enabled the participants to identify and take appropriate actions when receiving phishing emails (Insyirah, et al., 2024).

3. Methodology

This study employed a descriptive survey-based research methodology, to assess awareness level and public knowledge on cyber fraud among Universiti Teknologi MARA (UiTM) Sarawak diploma students. The respondents of this study were 171 diploma students from various programmes who took Computer and Information Processing (CSC134) course. This study employed a structured questionnaire exclusively tailored from Ying, et al. (2023) and Bijwaard (2020) for the purpose of collecting data. The questionnaire was divided into two main sections. The first section is mainly related to the respondents' demographic information, including gender, program and ethnicity. The latter section consists of questions to gauge the level of awareness and public knowledge based on the issue of cyber fraud. This section particularly includes items measuring the respondents' familiarity with cyber fraud concepts, terms, and scenarios. The data collection process was done online via Google Form. The data collected from the instrument were analysed using IBM SPSS software. The quantitative data were analysed using descriptive analysis which included standard deviations, mean scores frequencies and percentages.

4. Findings and Discussion

The IBM Statistical Package for the Social Sciences (SPSS) version 25.0 was utilised in order to carry out a descriptive analysis of the survey data. From the responses of 171 students registered into Computer and Information Processing (CSC134) course at UiTM Sarawak, a total of 170 responses are used for further analysis. The features of the dataset were summarised and interpreted based on frequency, percentage, mean score, and standard deviation. The questionnaire items exhibited good reliability, as reflected by Cronbach's alpha coefficient of $\alpha = 0.762$, exceeding the commonly accepted threshold of 0.70 for internal consistency. A descriptive analysis was conducted on a sample of 170 responses using SPSS version 25. Table 1 presents the frequencies and percentages of the student distribution in this study.

Table 1: Demographics of respondents (N=170)

Demographic	Label	Frequency	Percentage (%)
Gender	Male	39	22.9%
	Female	131	77.1%
Program	AM110	34	20.0%
	AS120	25	14.7%
	BA132	76	44.7%
	IC120	35	20.6%
Ethnicity	Bidayuh	15	8.8%
	Chinese	2	1.2%
	Iban	33	19.4%
	India	2	1.2%
	Malay	83	48.8%
	Melanau	12	7.1%
	Other	23	13.5%

Majority of the respondents were female (77.1%), while only 22.9% were male. In terms of academic programs, 44.7% of the respondents were enrolled in Diploma in Office Management and Technology (BA132), followed by 20.6% in Diploma in Halal Management (IC120), 20.0% in Diploma in Public Administration (AM110), and 14.7% in Diploma in Science (AS120).

Regarding ethnicity, nearly half of the respondents (48.8%) identified as Malay. Other significant ethnic groups included Iban (19.4%), Bidayuh (8.8%), and Melanau (7.1%). Smaller percentages were recorded for respondents of Chinese and Indian ethnicities, each at 1.2%, while 13.5% of the respondents identified as belonging to other ethnic groups.

Table 2: Awareness of Phishing and Macau Scams among Respondents

Items	Response	Frequency	Percentage (%)
Awareness of Phishing scams	Yes	92	54.1%
	No	78	45.9%
Awareness of Macau scams	Yes	114	67.1%
	No	56	32.9%

The study also examined the awareness among respondents regarding different types of cyber fraud, specifically phishing scams and Macau scams. As shown in Table 2, more than half of the respondents (54.1%) indicated that they were aware of phishing scams, while 45.9% reported that they were not aware of such scams.

In relation to Macau scams, a higher percentage (67.1%) of respondents reported familiarity compared to 32.9% who were not aware. These results suggest that the respondents had greater awareness of Macau scams compared to phishing scams.

Table 3: Mean Score Interpretation

Mean Score	Interpretation
1.00-1.80	Very Low
1.81-2.60	Low
2.61-3.20	Medium
3.21-4.20	High
4.21-5.00	Very High

Source: Moidunny (2009)

According to Moidunny (2009), the mean score interpretation is as shown in Table 3.

Table 4: Self-assessed knowledge of Phishing and Macau Scams among Respondents

Items	Mean	Standard Deviation	Level of Knowledge
Knowledge regarding Phishing scams	2.59	1.000	Low
Knowledge regarding Macau scams	2.71	1.113	Medium

Table 4 presents the self-assessed knowledge of respondents regarding Phishing and Macau scams. The mean score for knowledge regarding Phishing scams was M = 2.59 (SD = 1.000), categorized as Low. In comparison, the mean score for knowledge regarding Macau scams was slightly higher at M = 2.71 (SD = 1.113), categorized as Medium. These findings suggest that respondents perceived themselves as being slightly more knowledgeable about Macau scams than Phishing scams.

Table 5: Level of Agreement with Statements Regarding Cyber Fraud Awareness and Prevention

Items	Mean	Standard Deviation	Level of Agreement
I know the meaning of cyber fraud or online fraud.	3.56	0.856	High
I am aware that online scams are on the rise lately.	3.86	0.931	High
I know the level of awareness of online fraud prevention in Malaysia is very low.	3.61	0.931	High
I believe Malaysian society needs education about online fraud.	4.00	0.967	High
I know the cause of a person being deceived in online fraud.	3.56	0.863	High
I am aware of the main reason a person is deceived but does not call the police.	3.58	0.888	High
I know what to do after suffering a loss from an online scam.	3.36	0.958	High
I will accept payment from a party in exchange for allowing them to use my identification to open a bank account.	2.46	1.306	Low
If a friend recommends an online investment with a low credit but highly profitable, I will invest.	2.55	1.240	Low
I have received any fraud prevention publicity through any channels.	3.16	0.965	Medium
I think the level of anti-fraud publicity methods in Malaysia is low.	3.44	0.883	High
I think application methods should be used for anti-fraud publicity to be more awareness effective in the future.	3.62	0.883	High
If there is a comprehensive cyber fraud prevention application and focus on the Malaysian community, I will introduce it to my friends.	3.66	0.883	High

Table 5 presents the respondents' levels of agreement with various statements related to cyber fraud awareness and prevention. Overall, the findings indicate a high level of agreement with most of the statements. The mean scores for these statements ranged from 3.36 (SD = 0.958) to 4.00 (SD = 0.967), with the highest agreement recorded for the statement that Malaysian society needs education about online fraud (M = 4.00, SD = 0.967).

In contrast, a moderate level of agreement was observed for the statement concerning respondents' exposure to fraud prevention publicity through various channels, which recorded a mean score of 3.16 (SD = 0.965).

On the other hand, low levels of agreement were noted for two statements, suggesting respondents' general reluctance to engage in potentially risky or unethical behaviours. These included: "Accepting payment from a party in exchange for allowing the use of personal identification to open a bank account" (M = 2.46, SD = 1.306), and "Investing in an online scheme recommended by a friend, despite low credibility but high promised returns" (M = 2.55, SD = 1.240).

5. Conclusion

This study aimed to elucidate the understanding on the awareness level and knowledge of cyber fraud among diploma students at Universiti Teknologi MARA (UiTM) Sarawak. The findings indicated that more than half of the respondents have awareness and general knowledge of cyber fraud. Particularly the respondents indicated better awareness and knowledge in relation to Macau Scams than phishing scams. Overall, majority of the respondents agreed that the Malaysian public needs to be educated about online fraud, as the level of awareness of online fraud prevention in Malaysia remains low. However, this study also shows that respondents receive only moderate exposure to cyber fraud prevention publicity, and they also perceive that the level of fraud prevention publicity methods in Malaysia is low. Based on these findings, the study recommends introducing more targeted educational initiatives at all levels of society. As an attempt to educate the Malaysian public, efforts such as cyber security awareness programmes (Jalil, et. al. 2024), National Fraud Prevention Centre (NFPC) mobile application (Ying, et. al. 2023), Pendekar Siber web portal (Ismail, et. al. 2024), and Cyber Security Awareness Game (Shen et. al. 2021) could help. These initiatives provide news updates about recent fraud techniques, preventive measures against cyber fraud, and quizzes for testing knowledge regarding cyber fraud. In addition, effective fraud prevention publicity strategies and policy development are also necessary to overcome cyber fraud. Hence, all these initiatives are crucial in empowering the Malaysian public with the knowledge and skills necessary to identify and respond to cyber threats effectively.

References

Aljammal, A. H., Qawasmeh, A., Taamneh, S., Wedyan, F., Obiedat, M., & Salameh, H. B. (2024). Assessing cybersecurity awareness among the Hashemite University students in terms of computer usage. *2024 16th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)* (pp. 1-6). IEEE.

Astro Awani. (2024). *CyberSecurity rekod 5,181 insiden keselamatan siber setakat Oktober*. Retrieved from https://www.astroawani.com/berita-malaysia/cybersecurity-rekod-5-181-insiden-keselamatan-siber-setakat-oktober-496022.

Bijwaard, D., 2020. *Survey on "scams and fraud experienced by consumers" - final report*, European Institute for Gender Equality. Lithuania. Retrieved from https://coilink.org/20.500.12592/96n468 on 15 Jan 2025. COI: 20.500.12592/96n468.

Awodiran, M. A., Ogundele, A. T., Idem, U. J., & Anwana, E. O. (2023). Cybercrime consciousness among undergraduate students. *2023 International Conference on Cyber Management and Engineering (CyMaEn)* (pp. 301-306). IEEE.

Dewan Kosmik. (2025). *Malaysia paling terjejas di Asia Tenggara akibat serangan siber*. Retrieved from https://dewankosmik.jendeladbp.my/2025/01/05/15964.

Du, X., & Chintakovid, T. (2023). A Survey of Cybersecurity Awareness Among Undergraduate Students at Yunnan University of Finance and Economics in China. *2023 4th International Conference on Education, Knowledge and Information Management (ICEKIM 2023)*, (pp. 740-753). Atlantis Press.

Insyirah, N., Asokan, K., Singh, I., & Arumugam, D. (2024). The Impact of Cyber Security Culture on Malaysian Adults' Susceptibility to Phishing Emails in the Banking Sector. *Electronic Journal of Business and Management ICDBSE Special Issue, 122-138.*

Ismail, N. S., Ismail, S. A., & Molok, N. N. A. (2024) Pendekar Siber Portal: Empowering Malaysian Youth Through Cybersecurity Education. *Advancement in ICT: Exploring Innovative Solutions (AdICT),* (2), 39-46.

Jalil, M., Ali, N., Yunus, F., Zaki, F. A. M., Hsiung, L. H., & Almaiah, 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.

Majlis Keselamatan Negara (MKN). (2024). *Scammer kaut RM6 juta sehari di Malaysia*. Retrieved from https://www.mkn.gov.my/web/ms/2024/09/26/scammer-kaut-rm6-juta-sehari-di-malaysia.

Malaysia Computer Emergency Response Team (2024). *SR-027.092024: MyCERT Report - Cyber Incident Quarterly Summary Report - Q2 2024*. Retrieved from https://mycert.org.my/portal/advisory?id=SR-027.092024.

Moidunny, K. (2009). *The effectiveness of the national professional qualification for educational leaders (NPQEL)* [Unpublished doctoral dissertation]. Universiti Kebangsaan Malaysia.

Oyelakin, A. M. (2024). An investigation into the awareness level of university undergraduates on cyber incident reporting and response in Kwara State. *Malaysian Journal of Applied Sciences*, *9*(1), 1-9.

Pitchan, M. A., Omar, S. Z., & Ghazali, A. H. A. (2019). Amalan keselamatan siber pengguna Internet terhadap buli siber, pornografi, e-mel phishing dan pembelian dalam talian [Cyber security practice among internet users towards cyberbullying, pornography, phishing email and online shopping]. *Jurnal Komunikasi: Malaysian Journal of Communication*, *35*(3), 212-227.

Ting, T. T., Cheah, K. M., Khiew, J. X., Lee, Y. C., Chaw, J. K., & Teoh, C. K. (2024). Validation of cyber security behaviour among adolescents at Malaysia university: Revisiting gender as a role. *International Journal of Innovative Research and Scientific Studies*, *7*(1), 127-137.

Shen, L. W., Mammi, H. K., & Din, M. M. (2021, October). Cyber security awareness game (CSAG) for secondary school students. *2021 International Conference on Data Science and Its Applications (ICoDSA)* (pp. 48-53). IEEE.

Ying, L. X., Aman, A. H. M., Jalil, M. S., Omar T. M., Attarbashi, Z. S., & Abuzaraida, M. A. (2023). Malaysia Cyber Fraud Prevention Application: Features and Functions. *Asia-Pacific Journal of Information Technology and Multimedia*, 12(2), 312-327.