Jurnal 'Ulwan
eISSN: 2600-7843
Jilid 9 (Bil.1) 2024: 14-22

CYBERCRIME AWARENESS ON ONLINE SHOPPING AMONG UITM STUDENTS AT TERENGGANU CAMPUS

Nor Faezah Ghazi Ahmad*
Akademi Pengajian Islam Kontemporari,
Universiti Teknologi MARA (UiTM) Cawangan Terengganu
Kampus Dungun Sura Hujung,
23000 Dungun, Terengganu, Malaysia

Nuurul Farihah Mohd Rosly
Akademi Pengajian Islam Kontemporari,
Universiti Teknologi MARA (UiTM) Cawangan Terengganu
Kampus Dungun Sura Hujung,
23000 Dungun, Terengganu, Malaysia

**Corresponding Author's Email: norfaezahga@uitm.edu.my*

Article History:
Received : 16 February 2024
Accepted : 3 April 2024
Published : 25 Jun 2024

To cite this article:
Ahmad, N.F.G. & Rosly, N.F.M. (2023). Cybercrime Awareness on Online Shopping among UiTM Students at Terengganu Campus. *Jurnal 'Ulwan*, *9*(1), 14-22

ABSTRACT

In recent decades, the Internet has emerged as an essential element of our daily lives. The widespread reliance of individuals on the internet has substantially increased their vulnerability to cybercrime. The prevalence of cybercrime has become a substantial peril in modern society. This research aimed to examine the variables that are associated with the extent of cybercrime awareness among students enrolled at UITM Dungun. To achieve the objective, the research was centered on particular research objectives, which entailed examining the attributes of social media that influence the degree of cybercrime awareness among students enrolled at UiTM Terengganu. As a result, 116 students in total contributed to the successful completion of the research. The Statistical Package for the Social Sciences (SPSS Statistic 28.0.1.1 Windows) was utilised to gather the data. According to the results of this research, a considerable percentage of students demonstrated awareness and understanding of the concept of cybercrime. There is broad consensus regarding the substantial surge in cybercrime. In contrast, this issue can be effectively mitigated through the implementation of appropriate preventive measures. Users are advised to exercise caution when accessing the internet. The documentation and observation

of students can be achieved by conducting a range of educational activities, including seminars, workshops, and conferences.

Keywords: cybercrime, social media, online shopping, student, awareness

1.0 INTRODUCTION

In the present day, the virtual realm is devoid of any limitations. This is because the internet has an unlimited capacity for communication, which allows information to spread to other countries. Users from all nations have the liberty to publicly interact, exchange information, and participate in any online endeavour. Online shopping is often regarded as a thriving kind of e-commerce on the Internet due to its widespread adoption in modern society. This culture is rapidly proliferating due to their hectic daily routines and the convenience of online connectivity. According to Harian Metro (2022), Malaysia boasts the largest percentage of digital users, with 88 percent or 22 million individuals. Furthermore, it is projected that by the end of this year, 90 percent of consumers would have transitioned to utilising digital gadgets. According to him, there has been a 47% increase in online spending per person compared to the previous year, and he predicts that global e-commerce sales would grow by 1.3 times by 2026.

Despite the convenience and growth of the e-commerce lifestyle, there is still a significant risk. Online retailers are routinely targeted by cybercrime, such as financial fraud. According to Rosley et. al, (2023), cybercrime is a type of crime that involves the use of any kind of electronic device connected to the internet to perpetrate a crime, whether it involves one person or a group of individuals, and is capable of crossing international borders quickly and without any limits. According to the National Risk Assessment 2020, fraud and losses in the country grew between 2017 and 2020. Over 20,000 cybercrimes were reported in 2021 alone, resulting in losses of RM560 million. Malaysians lost around RM2.23 billion as a result of cybercrime between 2017 and July 2021. As more people utilise mobile devices to conduct online transactions, there will be an increase in online banking fraud employing mobile malware.

Fraud losses are still a small part of the total value of online banking transactions, but they show that risks are always there and changing as people get used to new ways of living and doing business. The fact is that scammers are taking advantage of how quickly technology is spreading these days. This pattern won't change. As a result, making the financial system stronger against new threats and weaknesses must remain a top goal.

The majority of online fraud cases arise due to insufficient community scrutiny. As of April 2022, the global number of internet users exceeds five billion, accounting for around 63.1 percent of the global population. This has sparked concerns regarding the susceptibility to online fraud in e-commerce. Out of the total global population, 59% or over 4.7 billion individuals utilised social media. According to Nuryanto (2014), women are more susceptible to cyber fraud. Salespeople who planned to employ students in locations where their sensitive personal information, such as bank account numbers or credit card details, could be

readily pilfered and accessed by hackers would find it simpler to deceive them. The pervasive influence of new media on all aspects of Malaysian society is indicative of the country's progress in statistics and communications. The Internet allows for the efficient and quick fulfilment of daily needs. According to Pitchan & Omar (2019), over 145% of Malaysians who own registered cell phones have accessed the Internet, accounting for about 69% of the entire population of the country. According to his assertion, a significant proportion of Internet users in Malaysia, specifically 68%, utilise social media platforms, with a particular focus on Facebook and Instagram. These findings indicate that a significant proportion of Malaysians presently depend on the Internet for their daily activities. Researchers have recently engaged in discussions regarding the safety concerns of Internet users. The rise in cybercrime occurrences, such as cyberbullying, pornography, phishing emails, and online purchase fraud, is the reason behind the increase in Malaysia.

This insight arises from the students' awareness of the characteristics of a university student, encompassing individuals who exhibit a profound curiosity and eagerness to explore novel experiences. The majority of individuals who make this observation are female students. This will effectively convince individuals to accept it as genuine and make choices without considering the repercussions. The primary aim of this study is to examine the relationship between the attributes of social media and cybercrime among UITM students.

2.0 LITERATURE REVIEW

2.1 Background of Cybercrime

Cybercrime has emerged as a constantly changing worldwide threat, fundamentally altering the nature of criminal activity in the era of digital technology. Cybercrime refers to a wide range of unlawful crimes carried out through computer systems and the internet, including but not limited to financial fraud, cyberbullying, and cyberspionage (Fuad et al., 2022). Cybercrime, as defined by Ghani & Ghazali (2021), encompasses any criminal activity carried out using the internet. Cybercrime encompasses various illicit activities such as financial fraud, unauthorised access to computer systems, password forgery, identity theft, and distribution of explicit material. Tracking down cybercriminals is challenging due to their utilisation of online platforms to carry out illegal actions.

Nowadays, cybercrime encompasses more than just using computers to commit crimes; it can also refer to crimes committed on the internet or in the online world that involve fraud and other forms of deception. The Malaysian Computer Emergency Response Team (MyCERT)'s next evolution will give reference and statistics services to the Malaysian community dealing with computer security issues (Esmail et al., 2018). Furthermore, unlike other physical crimes such as murder, theft, and stealing, cybercrime can sometimes be observed and identified by genuine criminals. This is a difficulty and a problem, especially when the offenders are situated outside Malaysia, because it can jeopardise the region's security efforts. Cyber fraud is considered tough to tackle. Cybercrime offers a huge risk to customers and is clearly a new millennium endeavour and crime, as opposed to murder, which can be proven with guns. In each case, cybercrime involves the use

of computer systems or electronic devices, and the prosecution includes a large number of participants, comparable to the number of experts.

2.2 Factors Influencing Social Media

Social media platforms play an important role in disseminating information and raising awareness about cybercrime. The publication of information about this criminal activity may spark a collective desire among the community to improve their skill in using information technology to reduce the risk of falling victim to cybercriminal operations. The transmission of instructional and instructive resources to the general public, particularly adolescents, can raise public awareness about the dangers associated with various types of cybercrime (Norman & Othman, 2020). As a result, incorporating full social media literacy into educational curricula is critical, with a focus on the younger generation.

Individuals of various age groups and genders are currently creating profiles on digital social platforms to establish connections within this virtual realm. Certain individuals own a substantial quantity of acquaintances and adherents across numerous profiles. Simultaneously, there has been a rise in the quantity of fraudulent accounts (Ganesh et al., 2020). Spurious profiles frequently inundate users by disseminating inappropriate or unlawful content. Fraudulent profiles are created by distorting the identity of a recognised person to torment them. As to the findings of Salleh and Ilham (2017), individuals who utilise social media platforms tend to disclose diverse personal information on the internet. Subsequently, individuals refrain from utilising some programmes on their smartphones and tablets due to apprehensions regarding the security and confidentiality of their online communication and information sharing. Unauthorised dissemination of personal records by users on the Internet or social media platforms can lead to detrimental outcomes, including identity theft, unauthorised access to records, and misuse of personal information. According to the survey, a significant majority of 78% of participants expressed that they no longer have any worries over the disclosure of private information through social media platforms. These are worrisome issues as they create openings for those who are not accountable for misusing a consumer's confidential information.

In modern society, social media serves a purpose that goes beyond its conventional role of enabling social connections. It has transformed into a platform that functions as a channel for distributing diverse information, tackling societal problems, and advocating religious values. The rapid growth of the digital realm has resulted in the gradual increase of a specific demographic, albeit with negative consequences for a country, especially within some sectors of the population. However, a substantial number of people are not sufficiently aware of the increased vulnerability of surfers to cyber threats, such as the unfortunate probability of becoming victims of online fraud, the compromise of personal information, and other similar dangers. Furthermore, it is essential to recognise the pivotal role of law enforcement in tackling cybersecurity issues (Pitchan & Omar, 2019). As mentioned before, the level of community awareness and the efficacy of law enforcement agencies might impact the frequency and successful resolution of cybercrime

incidents in Malaysia. Therefore, it is crucial to emphasise the need of raising awareness about cybercrime on social media platforms.

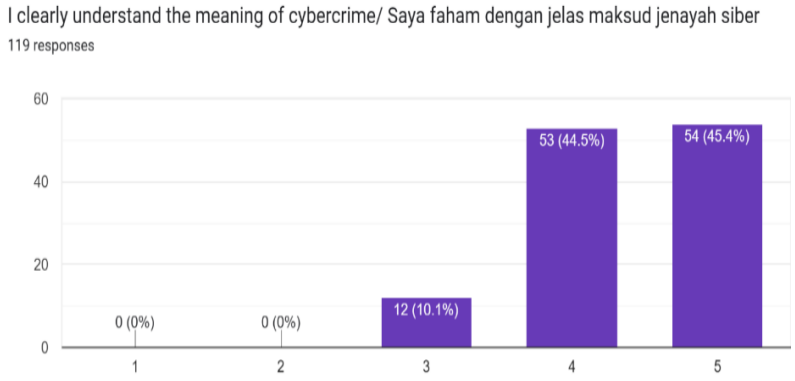
3.0 METHODOLOGY

The research methodology involves using a questionnaire distributed over a Google Form. The sample consists of 150 participants from the Universiti Teknologi Mara branch in Terengganu, aged between 18 and 25 years. This study aims to determine the elements that impact student preferences and the difficulties faced by UITM students when making online purchases. This study is appropriate for quantitative research as it effectively showcases the importance of sampling, designing, and administering questionnaires in collecting information from a specific group or population. The purpose is to conduct a systematic analysis to improve understanding of their behaviour and characteristics (Apuke, 2017).

The data collected from the questionnaire is analysed using the Statistical Package for the Social Sciences (SPSS Statistics 28.0.1.1 Windows). Data analysis software, such as SPSS, is widely used in research to perform thorough analysis, transformation, and summarising of data using tables and graphs. Inferential statistics involve a range of statistical methods, such as regression models, analysis of variance, and factor analysis. In addition, basic descriptive statistics, such as measures of central tendency (for example, averages) and measures of dispersion (such as frequencies), are also taken into account in this field. Multiple instruments can be employed in conjunction with SPSS to alter data. These tools include functions that allow for data recording, variable calculation, and data combining and aggregation (Zou et.al, 2019).

4.0 FINDING

The purpose of this section is to assess the general comprehension and knowledge of cybercrime among the student at UiTM Terengganu.



Graph 1
The Level of cybercrime awareness among UITM students

Graph 1 displays the frequency distribution and proportion of participants' awareness of cybercrime. Out of the entire sample of 104 students, a significant majority (89.6%) displayed a clear understanding of the concept of cybercrime. The percentage of participants that are unaware of this cybercrime, specifically 12 persons, is then depicted as 10.3%. The finding suggests that the students at UITM have a substantial level of awareness and understanding when it comes to cybercrime.

4.1 The level of cybercrime awareness among UITM students.

This section refers to the extent of cybercrime awareness among UITM students. The matter is represented in Table 1.

Table 1: The Level of Cybercrime Awareness Among Students at UITM

Descriptive Statistics

	N	Range	Minimum	Maximum	Sum	Mean		Std. Deviation
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic
B1- I clearly understand the meaning of cybercrime/ Saya faham dengan jelas maksud jenayah siber	116	2.00	3.00	5.00	504.00	4.3448	.06135	.66074
B2- In my opinion, the increasing cases of cybercrime in Malaysia are cause for concerned/ Pada pendapat saya, kes jenayah siber yang semakin meningkat di Malaysia membimbangkan	116	3.00	2.00	5.00	518.00	4.4655	.06175	.66504
B3- I am the victim of cybercrime/ Saya adalah mangsa jenayah siber	116	4.00	1.00	5.00	253.00	2.1810	.11655	1.25524
B4- Fraud/ Penipuan	116	2.00	3.00	5.00	522.00	4.5000	.05677	.61148
B5- Information theft/ Kecurian maklumat	116	2.00	3.00	5.00	534.00	4.6034	.05031	.54181
B6- Data Theft/ Kecuarian data	116	3.00	2.00	5.00	533.00	4.5948	.05334	.57451
B7- Hacking/ Menggodam	116	2.00	3.00	5.00	537.00	4.6293	.04978	.53617
B8- If I am the victim, I will report it to the authority/ Jika saya menjadi mangsa, saya akan melaporkannya kepada pihak berkuasa	116	2.00	3.00	5.00	505.00	4.3534	.06845	.73726
B9- Lack of knowledge/ Kurang pengetahuan	116	4.00	1.00	5.00	486.00	4.1897	.08021	.86390
B10- Lack of awareness/ Kurang kesedaran	116	4.00	1.00	5.00	476.00	4.1034	.08339	.89811
B11- Not bothered/ Tak ambil peduli	116	4.00	1.00	5.00	470.00	4.0517	.08985	.96769
B12- Don`t know how to report it/ Tidak tahu bagaimana untuk melaporkannya	116	4.00	1.00	5.00	521.00	4.4914	.07086	.76324
B13- Shame/ Malu	116	4.00	1.00	5.00	484.00	4.1724	.09506	1.02385
Valid N (listwise)	116							

All the questions were reported with high mean values based on Table 1, except for question 3 which is (M = 2.1810, SD = 1.25524), which registered a moderate mean value. Question 7 showed the highest mean value (M = 4.6293, SD = 53617), Question 5 (M = 4.6034, SD = 54181) was the second highest, while

Question 6 reported the third highest mean value relative to other questions, including Question 4 (M = 4.5000, SD = 61148), Question 12 (M = 4.4914, SD = 76324), Question 2 (M = 4.4655, SD = 66504), Question 8 (M = 4.3534, SD = 73726), Question 1 (M = 4.3448, SD = 66074), Question 9 (M = 4.1897, SD = 86390), Question 13 (M = 4.1724, SD = 1.02385), Question 10 (M = 4.1034, SD = 89811), Question 11 (M = 4.0517, SD = 96769). These findings indicate that the students are aware of the increasing prevalence of cybercrime in our country.

4.2 The Media Social Factors that Influence User's Awareness of Cybercrime Among UITM Students

This section refers to the media social factors that can influence students' awareness of cybercrime among UITM students. The matter is stated in Table 2.

Table 2: The Media Social Factors That Influence Users' Awareness of Cybercrime Among UITM Students

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
E1- Instagram	116	1.00	5.00	4.4483	1.38529
E2- Tiktok	116	1.00	5.00	4.1724	1.62735
E3- Youtube	116	1.00	5.00	4.1034	1.67529
E4- Facebook	116	1.00	5.00	2.5517	1.95757
E5-Shopee	116	1.00	5.00	3.3103	1.98435
E6- Lazada	116	1.00	5.00	1.5172	1.34800
E7- Other	116	1.00	5.00	1.4138	1.22346
E8- How long do you use social media in a day?/ Berapa lamakah tempoh anda menggunakan media sosial dalam sehari?	116	1.00	4.00	2.3103	.77363
E9- Online shopping/ Membeli-belah dalam talian	116	1.00	5.00	4.3448	1.48677
E10- Looking for friends/ Mencari kawan	116	1.00	5.00	2.7241	1.98948
E11- Online business/ Perniagaan Online	116	1.00	5.00	1.6897	1.51751
E12- For education (discussion)/ Pendidikan (Perbincangan)	116	1.00	5.00	4.2759	1.54687
Valid N (listwise)	116				

All inquiries exhibited a significantly elevated average score as indicated in Table 2, except inquiry 7, which yielded a moderately lower mean value (M = 1.4138, SD = 1.22346). Question 1 exhibited the highest mean value (M = 4.4483, SD = 1.38529), followed by Question 9 (M = 4.3448, SD = 1.48677) as the second highest. Question 12 reported the third highest mean value compared to other questions, including Question 2 (M = 4.1724, SD = 1.62735), Question 3 (M = 4.1034, SD = 1.67329), Question 5 (M = 3.3103, SD = 1.98435), Question 10 (M = 2.7241, SD = 1.98948), Question 4 (M = 2.5517, SD = 1.95757), Question 8 (M =

2.3103, SD = 77363), Question 11 (M = 1.6897, SD = 1.51751), and Question 6 (M = 1.5172, SD = 1.34800). The data indicates that social media has an impact on users' perception of cybercrime. In modern times, a considerable number of students dedicate a large portion of their time to interacting with social media platforms, resulting in an increased knowledge of current events and news primarily through these digital channels. Therefore, the influence of social media on students can be seen as advantageous.

5.0 CONCLUSION

In conclusion, the researchers found that the majority of students reported never experiencing cybercrime due to their highly vigilant approach to sharing information on social media. Nevertheless, a total of 19 students have fallen prey to cybercrime as a result of the individual's carelessness. The predominant actions taken thus far have involved filing a formal complaint with the authorities and employing internet blocking measures to prevent further harassment. Moreover, the research revealed that academics choose to allocate their time on social media platforms like Instagram, TikTok, YouTube, Shopee, and others to purchase things online, particularly when the platform lacks commercial recognition. It is crucial to raise knowledge of cybercrime among Malaysian Internet users, including both younger individuals such as students and older individuals. To address this issue, students should prioritise enhancing their self-awareness to remain vigilant towards the increasing prevalence of cybercrime incidents.

The exponential expansion of cybercrime exceeds that of all other types of illicit behaviour, presenting a substantial peril to the welfare of our country. Moreover, this finding implies that individuals of all genders are cognizant of the increasing frequency of cybercrime. However, its occurrence can be mitigated through the adoption of effective preventive measures and the implementation of suggested strategies. Preventing rather than treating underscores the importance of increasing awareness regarding the hazards linked to internet usage, as it is critical that all individuals are well-informed. Finally, it is significant to mention that the pervasive adoption of the internet among millions of Malaysians has resulted in the rise and continuous development of cybercrime, an ever-present menace. It is imperative to possess a thorough comprehension of every facet of cybercrime so as to provide assistance to law enforcement and government entities and to raise public consciousness concerning these unlawful undertakings. Implementing this measure could potentially reduce the occurrence of cybercrime and improve the ability of the general public to safeguard themselves against fraudulent activities, which could encourage participation in such unlawful activities.

Author Contributions

Ahmad, N.F.G., Abstract and content. Rosly, N.F.M., has been a co-author and has analyzed the research findings in this manuscript.

Conflicts Of Interest

The manuscript has not been published elsewhere and is not under consideration by other journals. All authors have approved the review, agree with its submission and declare no conflict of interest on the manuscript.

REFERENCES

Apuke, O. D. (2017). Quantitative research methods: A synopsis approach. *Kuwait Chapter of Arabian Journal of Business and Management Review*, 33(5471), 1-8.

Esmail, N. K., Hassan, R. A., Karto’ On, Z. A. A., & Kamaruddin, N. A. (2018). *Hubungan Antara Jenayah Penipuan Internet dengan Pengurusan Produktiviti Pekerjaan.* Universiti Malaysia Sabah.

Fuad, N. S. M., Daud, M., & Yusof, A. R. M. (2022). Memahami Jenayah Siber Dan Keselamatan Siber Di Malaysia: Suatu Pemerhatian Terhadap Pandangan Sarjana Dan Intelektual: Understanding Cybercrime and Cybersecurity in Malaysia: An Observation from The Perspective of Scholars and Intellectuals. *Asian Journal of Environment, History and Heritage*, 6(1).

Ganesh, S., Ganapathy, D., & Sasanka, K. (2020). Awareness of Cyber Crime on Social Media. *Journal of Contemporary Issues in Business and Government*, 26(2)

Ghani, N. M., & Ghazali, S. (2021). Impak media sosial terhadap gangguan seksual atas talian dalam kalangan wanita muda.

Jenayah siber: 11,367 Kes Jenayah Siber Dalam Tempoh Tujuh Bulan. (2022, October 21). Hmetro.com.my. https://www.hmetro.com.my/mutakhir/2022/08/868599/11367-kes-jenayah-siber-dalam-tempoh-tujuh-bulan

Nuryanto, N. (2014). Aplikasi EDI (Electronic Data Interchange) Sebagai Wujud Pengembangan Pemberdayaan UMKM Furniture di Jawa Tengah. *Semantik*, 4(1).

Norman, A. A., & Othman, N. (2020). Ketagihan pornografi dalam kalangan remaja: Faktor dan implikasi terhadap sahsiah diri remaja. *Jurnal Melayu*, 19(2), 205-215.

Pitchan, M. A., & Omar, S. Z. (2019). Dasar keselamatan siber Malaysia: Tinjauan terhadap kesedaran netizen dan undang-undang. *Jurnal Komunikasi: Malaysian Journal of Communication*, 35(1), 103-119.

Rosley, N. A., Hashim, H., & Jen-T’Chiang, N. Z. C. (2023). Combating the Macau Scam in Malaysia: Strategies for Mitigation and Resolution from Civil Law and Sharī'ah Perspectives. *Law, Policy, and Social Science*, 2(2), 30-44.

Salleh, M. A. M., & Ilham, N. M. M. (2017). Pengalaman dan kesedaran pengguna dewasa terhadap isu pengawasan di media sosial. *Jurnal Komunikasi: Malaysian Journal of Communication*, 33(1), 502-514.

Zou, D., Lloyd, J. E., & Baumbusch, J. L. (2019). Using SPSS to analyze complex survey data: a primer. *Journal of Modern Applied Statistical Methods*, 18.