Jurnal ‘Ulwan
eISSN: 2600-7843
Jilid 10 (Bil.2) 2025: 140-156

CYBERSECURITY AWARENESS LEVELS IN THE DIGITAL AGE: A STUDY OF UNIVERSITY STUDENTS

Mohd Fazzly Rassis Md Kasim*
Faculty of Management and Informatics,
Sultan Ahmad Shah Pahang Islamic University (UnIPSAS),
KM 8 Jalan Gambang, 25150 Kuantan, Pahang Darul Makmur, Malaysia.

Wan Hashridz Rizal Wan Abu Bakar
Faculty of Da’wah, Education and Islamic Civilization,
Sultan Ahmad Shah Pahang Islamic University (UnIPSAS),
KM 8 Jalan Gambang, 25150 Kuantan, Pahang Darul Makmur, Malaysia.

Zuraini Mohamad @ Abdul Rahman
Faculty of Management and Informatics,
Sultan Ahmad Shah Pahang Islamic University (UnIPSAS),
KM 8 Jalan Gambang, 25150 Kuantan, Pahang Darul Makmur, Malaysia.

Zarina Kamarozaman
Faculty of Management and Informatics,
Sultan Ahmad Shah Pahang Islamic University (UnIPSAS),
KM 8 Jalan Gambang, 25150 Kuantan, Pahang Darul Makmur, Malaysia.

**Corresponding Author’s Email: fazzly@unipsas.edu.my*

Article History:
Received : 26 August 2025
Accepted : 14 November 2025
Published : 24 December 2025
© Penerbit Universiti Islam Melaka

To cite this article:
Md Kasim, M. F. R., Wan Abu Bakar, W. H. R., Mohamad, Z. & Kamarozaman, Z. (2025). Cybersecurity Awareness Levels In The Digital Age: A Study Of University Students. *Jurnal 'Ulwan, 10*(2), 140-156.

ABSTRACT

This study investigates university students' cybersecurity awareness in the context of increasing digital threats. As one of the most active user groups in cyberspace, students' level of knowledge is crucial to ensure online safety and reduce human-related vulnerabilities. Using a cross-sectional survey design and convenience sampling, data were collected from 142 respondents through a five-point Likert scale that assessed their familiarity with cybersecurity practices and terminology. The analysis revealed a high overall awareness level (Mean = 4.656, SD = 0.792), particularly among students aged 18–24. However, slightly lower awareness was *observed among those aged 25–34, indicating the need for targeted educational efforts. While the findings offer valuable insights, the limited sample size restricts the generalizability of the results. Therefore, future studies should include a more diverse and extensive sample to reflect broader trends. The study underscores the importance of practical training and age-responsive cybersecurity programs to strengthen digital resilience among university students.*

Keywords: *Cybersecurity, Level of awareness, University Student*

1.0 INTRODUCTION

Cybersecurity has emerged as an essential matter in our contemporary world, as the heightened reliance on internet technologies has instigated a surge in cyber hazards that may impact individuals, firms, and governments. The intricacy and advancement of cyber threats have intensified, presenting considerable obstacles to global security. The risks involve internet crimes, secretive cyber spying, and acts of cyber terror, potentially resulting in severe impacts on economic processes, vital infrastructure, and the security of the nation. The transnational character of these threats necessitates collaborative international efforts and the formulation of comprehensive cybersecurity frameworks to safeguard against prospective assaults.

The proliferation of cybersecurity challenges is intensifying globally, significantly influencing international diplomatic relations. The swift technological progress characteristic of the 21st century demands the establishment of high-calibre cybersecurity frameworks across all nations, necessitating considerable financial resources, skilled personnel, and specialized training programs. The annual increase in cybercriminal activities contributes to a pervasive psychological insecurity among the populace. Assertive nation-states, exemplified by Russia, capitalize on cyberspace to gain geopolitical leverage, especially in contexts of conflict such as the Russia-Ukraine war, thereby highlighting the pressing necessity for comprehensive cybersecurity strategies on a global level (Guchua & Zedelashvili, 2023).

According to Tanwar (2025), the global landscape of cybersecurity challenges encompasses the escalating complexity and frequency of cyber threats, which include malware, phishing schemes, ransomware, and advanced persistent threats. These malign entities target both individuals and organizations, thereby necessitating the implementation of robust cybersecurity protocols. A comprehensive, multifaceted security framework is imperative, which integrates technological solutions such as firewalls and encryption, establishes policy frameworks for adopting best practices, and addresses human behavioural factors through ongoing education and awareness initiatives. The ever-evolving character of these threats mandates proactive and adaptable strategies to bolster defensive measures effectively.

Ahmad et al. (2024) posited that cybersecurity has emerged as a paramount concern within Malaysia's maritime sector, attributable to many cyber intrusions that have resulted in considerable financial detriment and the illicit appropriation of sensitive data. The discourse accentuates the imperative for cybersecurity preparedness among maritime stakeholders, delineating organizational and contextual variables as pivotal determinants that shape this preparedness. The investigation highlights the pressing necessity for the maritime industry in Malaysia to implement robust cybersecurity protocols to alleviate the risks associated with such threats.

A scholarly examination conducted by Pillay and Gowindasamy (2025) indicates that Malaysia encounters formidable challenges in cybersecurity, particularly concerning the governance of cybersecurity practices. It underscores the need for an in-depth comprehension of the intricate interactions among individuals, procedures, and technologies to tackle these challenges proficiently. The research posits that adopting a human-centric design in cybersecurity frameworks and ensuring the congruence of local procedures with technological capabilities are imperative for enhancing cybersecurity governance. This methodology is vital for formulating resilient defences against the continuously evolving cyber threats within the Malaysian context.

The issue of cybersecurity within Malaysia, particularly in the context of the COVID-19 pandemic, encompasses a heightened prevalence of cyber fraud that predominantly targets at-risk populations, notably individuals aged 60 years and older. Many elderly individuals exhibit a deficiency in cybersecurity awareness, rendering them particularly vulnerable to phishing scams and malware attacks. Although a portion of civil service respondents demonstrates some level of awareness, there persists a notable ambiguity regarding the operational methods employed by cybercriminals and the relevant privacy legislation governing the dissemination of personal, financial, or medical information, thereby underscoring an urgent necessity for the enhancement of cybersecurity education and the establishment of robust policy frameworks (S. L. Tan et al., 2020).

The inadvertent revelation of confidential information constitutes a considerable cybersecurity challenge within Malaysia's banking sector. Such vulnerabilities may culminate in cyber assaults and client attrition and ultimately affect financial performance. The insufficiency of extensive security protocols and a deficit of awareness among personnel intensify these challenges, thereby underscoring the imperative for an ingrained culture of cybersecurity awareness and comprehensive training initiatives to safeguard critical data from larceny and exploitation (Krishnan et al., 2023).

In the modern era, where the digital presence can be secluded yet achieve vast integration instantly, the rubble of practice needs to acknowledge the need for cybersecurity awareness. Organizations across several domains have frequently established such programs for employees capable of addressing and solving the issues arising from various cybersecurity threats. These moves have resulted in many people needing more scientific awareness about their cyber activities. Reasons contributing to this trend include poor training implementation, old-fashioned content, and sloppy marketing strategies. As Alharbi and Tassaddiq (2021) observe, many training solutions need to relate better with employees, so a considerable gap remains in their comprehension of such cybersecurity practices and protocols.

In particular, students at the university level do not exhibit any cyber awareness, which is alarming. Alqahtani (2022) states that these students are only given a fundamental knowledge of cybersecurity, which makes it essential to address the gap in cyber education for students. Research indicates that students tend to regard the risks and threats of the Internet as dramatically low and do not comprehend the importance of prudent things like password creation, phishing, and safe browsing protocols.

The cybersecurity challenges in Malaysia are marked by a significant deficiency in awareness among the populace, especially among students of institutions of higher learning who, despite their frequent engagement with the Internet, possess insufficient knowledge to mitigate cyber threats effectively. Empirical evidence suggests that a staggering 99% of successful cyberattacks within the nation can be traced back to human errors. In light of this, the Malaysian government has instituted various initiatives, policies, and legislative measures designed to address these cybersecurity challenges and safeguard users from imminent threats (Ariffin & Letchumanan, 2020).

Students enrolled in Malaysian higher education institutions encounter considerable challenges with cybersecurity, primarily attributable to a deficient awareness and comprehension of cybersecurity threats. This deficiency in visibility and public cognizance exacerbates a digital divide in cybersecurity knowledge, behavioural practices, and attitudes amongst the student population. The findings stress the urgent need for uniform cybersecurity guidelines in educational settings focused on raising students' consciousness and readiness regarding cyber risks. This can ultimately uplift their livelihoods while contributing favourably to national cybersecurity goals (Ramakrishnan et al., 2022).

Faith et al. (2020) found that tertiary institution students in Malaysia encounter considerable cybersecurity challenges attributable to their continual engagement with the Internet. The research underscores that this demographic often constitutes the most vulnerable element in cybersecurity, with many factors impacting their cybersecurity-related behaviours. An investigation encompassing 450 students demonstrated that elements such as Perceived Vulnerability, Security Self-Efficacy, and Peer Behavior significantly correlate with their cybersecurity practices, thereby underscoring the imperative for augmented cybersecurity education and awareness within academic institutions to alleviate these issues.

Given these findings, this research paper is focused on examining the extent of the level of cybersecurity awareness among university students. By identifying the various gaps in knowledge and understanding, this study aims to enhance further the educational strategies employed so that students can keep themselves safe in a relatively unsecured cyberspace.

Cybersecurity awareness among university students constitutes a paramount area of inquiry in an increasingly digitalized society. Despite their status as some of the most prolific consumers of technological resources, students frequently lack the knowledge and comprehension necessary to navigate the complexities of cyberspace securely. This discrepancy between technology usage and cybersecurity awareness engenders substantial vulnerabilities, rendering students particularly susceptible to cyber threats, including phishing, malware, and data breaches. Investigating their level of cybersecurity awareness is imperative for identifying deficiencies and formulating targeted strategies to remediate them.

The significance of this research is further underscored by the reality that a considerable proportion of cybersecurity incidents stem from human error. When students are inadequately equipped to recognize and respond to cyber threats, they inadvertently transform into precarious links within the larger digital security framework. Enhancing cybersecurity awareness at the university level makes it feasible to mitigate the probability of such errors and bolster overall cybersecurity resilience.

Furthermore, university students epitomize the forthcoming workforce and leadership of the nation. Their digital behaviours and practices will substantially shape how organizations, institutions, and communities address cybersecurity challenges in the foreseeable future. Ensuring that students possess comprehensive knowledge and cybersecurity awareness will significantly contribute to establishing a more secure digital landscape at both organizational and national strata.

Additionally, this study holds considerable importance for formulating effective cybersecurity education programs. Gaining insights into students’ current levels of awareness facilitates the creation of pertinent, engaging, and pragmatic training initiatives. Such endeavours can effectively bridge the existing divide between theoretical knowledge and practical application, ensuring that students grasp cybersecurity principles and integrate them into their everyday conduct.

Investigating cybersecurity awareness among university students is crucial for diminishing cyber risks, averting data breaches, and fostering a culture of digital responsibility. It serves as a foundational pillar for establishing long-term security in an environment where digital threats are constantly evolving and expanding.

While existing literature has explored cybersecurity issues at national and sectoral levels, limited empirical attention has been paid to the awareness levels among university students in Malaysia. This demographic is particularly vulnerable due to high internet usage yet often lacks formal cybersecurity training. Therefore, this study aims to address this gap by assessing the extent of cybersecurity awareness among university students using a structured survey approach. Understanding this can inform the design of targeted educational programs and policy interventions.

2.0 PROBLEM STATEMENT

In the digital age, today’s students rely on online platforms for learning, socializing, gaming, and daily payments. This growing reliance leaves them vulnerable to a variety of cyberattacks, including phishing, malware data hacking, identity theft, and social engineering. While students use advanced technology in their daily work, many students still do not fully understand even the most basic cybersecurity principles, which puts them at risk and in danger of compromising their personal data, academic integrity, and digital health.

According to Alqahtani, (2022) stated that among students, they are generally only exposed to very basic cybersecurity knowledge, which emphasizes the need to strengthen and expand cybersecurity education for students. Although educational organizations have begun to introduce digital security modules and cyber awareness programs in schools, there is still a significant gap between students' level of awareness of technology and their level of cyber literacy. Unfortunately, many students do not consider cyber risks as something serious or assume that they will not become victims. As a result, various risky behaviors such as using weak passwords, careless sharing of personal information, and downloading files without verification are still widespread. This situation shows that there is a clear difference between the basic knowledge possessed by students and the level of cyber awareness required to ensure that they can safely explore the digital space.

Given these challenges, it is important to assess the actual level of cybersecurity awareness among students to identify weaknesses, behavioral patterns, and areas that require intervention. Without a clear understanding of students’ knowledge and practices, institutions may find it difficult to design truly effective training programs or policies to address real-world cyber risks. Therefore, this study examines students’ cybersecurity awareness levels to provide empirical evidence that can support the development of more focused, relevant, and effective cybersecurity education initiatives.

3.0 LITERATURE REVIEW

Moro-Visconti and Cesaretti (2023) define cybersecurity as the structured attempt to secure computer systems, networks, and data from illegitimate access, theft, damage, disruption, or cyber menace. This aspect involves realising various initiatives, regulations, technologies, and practices that protect the confidentiality, integrity, and availability of both information and systems. By addressing potential vulnerabilities and threats, cybersecurity assumes a pivotal role in protecting sensitive information and preserving the overall security of digital environments.

Cybersecurity covers the processes and practices intended to protect the equipped and interconnected devices, networks, and information linked through the Internet. , it aims to prevent unauthorized access whilst providing security for data in terms of confidentiality, integrity, and availability in the long run (Ujjwal Rao, 2023).

The chronicle of cybersecurity represents a multifaceted narrative that intricately weaves together technological progress, the emergence of evolving threats, and the reactions of diverse stakeholders, encompassing governmental entities, corporate organizations, and private individuals. From its formative phases in the 1960s with the introduction of time-sharing systems to the intricate cyber threats prevalent in contemporary society, cybersecurity has ascended to paramount importance within global security and economic resilience. The progression of cybersecurity epitomizes the dynamic interaction between technological advancements and the relentless endeavours of malevolent agents, thereby necessitating ongoing adaptation and strategic foresight by those entrusted with the protection of digital assets.

The idea of protecting computer networks began to develop in the 1960s, aligning with the introduction of time-sharing platforms, which demanded the defence of shared assets against unauthorized access (Yost, 2015). The 1970s witnessed the inception of cybersecurity studies as an independent discipline spurred by hacking and computer intrusions (Tarhan, 2022).

The implementation of the Department of Defense's Trusted Computer System Evaluation Criteria (TCSEC), commonly referred to as the Orange Book, in the 1980s, represented a pivotal advancement in the formulation of security standards; however, its inherent complexity ultimately resulted in its supersession by the more accessible international Common Criteria in the 1990s (Yost, 2015).

The decades of the 1980s and 1990s marked a substantial uptick in cyber offences, which thus brought about increased scrutiny over software and network security measures. This epoch was characterized by the emergence of hacking as a significant issue, resulting in the formulation of more sophisticated security protocols (Middleton, 2017). The cyberattacks on Estonia in 2007 underscored the susceptibility of essential infrastructure to cyber threats, thereby instigating a worldwide reevaluation of cybersecurity methodologies and emphasizing the necessity of safeguarding national and international networks (Tarhan, 2022).

Corporations have assumed a pivotal role in the evolution of cybersecurity, frequently navigating the intricate balance of cooperative and adversarial interests with governmental entities. Their engagement has become increasingly multifaceted as they face the dual challenges of safeguarding their proprietary assets while contributing to overarching security initiatives (Ning, 2022).

Nation-states have progressively acknowledged cybersecurity as an essential element of national security, precipitating comprehensive strategies and policies to alleviate cyber threats. This encompasses defensive and offensive strategies to safeguard against external and internal vulnerabilities (Subramanian, 2020).

Cybersecurity's growth in the Malaysian landscape has been marked by the quick evolution of technology and internet use since the early 1990s, especially following the creation of the Multimedia Super Corridor (MSC) in 1996. This initiative was designed to augment the accessibility of information technology and cultivate a conducive digital ecosystem. Nonetheless, Malaysia has encountered considerable cybersecurity challenges, encompassing cyber-attacks amidst international disputes, exemplified by the Ambalat Block conflict with Indonesia, which underscores the weaknesses present in its cyber infrastructure and underscores the imperative for enhanced security protocols (Othman, 2020).

According to Tan et al. (2020), the domain of cybersecurity within Malaysia has undergone significant transformation since the establishment of cyber legislative frameworks in 1997, which were instituted to combat the increasing prevalence of cybercriminal activities concomitant with the proliferation of information and communication technologies. The Malaysia Computer Emergency Response Team documented a total of 10,699 incidents in the year 2018, with fraudulent activities and intrusion attempts constituting the majority of these occurrences. Fundamental legislative measures include the Computer Crimes Act 1997, the Copyright (Amendment) Act 1997, the Communications and Multimedia Act 1998, and the Personal Data Protection Act 2010, all of which play a pivotal role in the legal prosecution of cybercriminals.

The initiation of the National Cyber Security Policy (NCSP) represents a strategic response to the escalating cyber threats, especially following the nation's Vision 2020 initiative, which was designed to foster a knowledge-based economy. The NCSP has been instituted to safeguard the Critical National Information Infrastructure (CNII) and has necessitated collaboration among various governmental ministries and agencies to enhance the cybersecurity framework of Malaysia over the preceding four years (Hashim, 2011).

Despite the rollout of numerous legal structures and policy efforts focused on improving the general cybersecurity situation, the degree of cybersecurity knowledge within the Malaysian community is still shockingly low, as human error has emerged as a key factor influencing the success of countless cyberattacks. In response to this pressing issue, the Malaysian government has embarked on the launch of a diverse array of programs meticulously designed to enhance public awareness regarding cybersecurity matters and to furnish users with the necessary protections against an increasingly complex and evolving spectrum of cyber threats (Ariffin & Letchumanan, 2020).

The extent of global cybersecurity awareness exhibits considerable variability among diverse demographics, geographical regions, and sectors. Such awareness is imperative as it directly affects the capacity to thwart and react to cyber threats. Empirical research suggests that although there is an increasing acknowledgement of the significance of cybersecurity, considerable deficiencies in knowledge and practices persist that necessitate rectification.

Empirical studies indicate that cybersecurity awareness is predominantly moderate to elevated within specific demographics, such as educational administrators in the Jazan region, yielding an average awareness metric of 3.48 on a scale of 5 (Otaif, 2023). Conversely, within the population of students and youthful social media participants, a notable deficiency in awareness is prevalent, exacerbating their susceptibility to cyber threats (Al Affan et al., 2025).

The link between education and awareness of cybersecurity practices is clear and important, indicating that as educational levels rise, so does one's comprehension of the intricate details and challenges within cybersecurity. It has been observed that individuals who possess higher levels of formal education are more inclined to exhibit superior awareness and engage in more effective cybersecurity practices that mitigate risks and enhance their overall digital safety (Nimkar & Kumar, 2024).

The comprehension of cybersecurity within the ranks of decision-makers is affected by various components, incorporating personal qualities such as gender, age, and the extent of their familiarity with information technology and cybersecurity strategies. The research indicated that male decision-makers demonstrated elevated levels of awareness compared to their female counterparts, with experience in information technology as the most pivotal factor correlated with awareness. Furthermore, organizational determinants, particularly the specific role assumed within the organization, contributed to this awareness. In contrast, the size of the organization and formal educational qualifications were not found to be significant in influencing cybersecurity awareness (Vrhovec & Markelj, 2024).

In particular, the area of cybersecurity deals with preventing intrusion by unfriendly forces in cyberspace, “actors” of no particular physical place with an intent to access, corrupt, or erase important databases, networks, and systems (M P, 2023). Many measures are employed to address these threats, including firewalls, encryption, firm password policy, and threat detection systems. These components are key to cybersecurity, thus demonstrating the necessity for a directed approach to the control and response of cyber threats (Mijwil et al., 2023). Recent studies by Al Kabir & Elmedany (2022) and Lee & Yim (2020) highlight the significance of password protection as part of cyber security measures, albeit its weaknesses.

However, the issue of password recycling, which is standard practice, poses a considerable risk to the security of even advanced systems. Besides passwords, several elements like social media activities such as Zoom and potential phishing schemes help identify cybersecurity myths. In this way, invalid claims and targeted operations about security are removed from a security system and its processes, thus improving them (Singhal et al., 2023). Most recently, Sufi (2023) cited in his work that AI and NLP can help cross social media information with national databases that have gaps and anomalies, thereby increasing the level of the country's cyber warfare and intelligence efficiently. Posting spam about threats to cybersecurity on social networks, particularly misinformation such as that put forward by. Hai-Jew, (2019), are key areas of concern. Research results demonstrate low and moderate rates of information imbalance concerning phishing web pages and Zoom system loopholes across various networks. Therefore, this justifies using social media for recruitment, detection of threats, and combating cybersecurity misinformation. Another key component of cybersecurity is ensuring browser security, which includes measures like preventing cross-site scripting attacks and browser leakage of private information (Yang et al., 2013). Similarly, Garcia and Bongo (2022) have shown that people who have taken ICT courses practice reasonably well in the protection of their data as well as avoiding unsafe applications. In contrast, Berry (2023) suggests that many students find it challenging to set the appropriate security features for their browsers because they do not understand the basic security principles.

In conclusion, the area of password protection, the use of social media in seeking threats, and the security of browsers constitute key variables in assessing the level of awareness regarding the issue of cybersecurity. If these areas are attended to, individuals and organizations can significantly improve their ability to protect critical information and systems from cyberattacks. Knowledge of these elements cultivates security as part of organizational culture and enables users to identify and reduce risks. As the advancing security threats and strategies evolve, the three elements considered in the study will be key in ensuring strength against new threats and a safe cyberspace.

Knowledge has been recognized as the primary determinant affecting cyber security awareness. The study underscores that, notwithstanding their status as digital natives, students exhibit insufficient knowledge and do not perceive themselves as secure within the cyber domain, consequently engaging in risky behaviours. Additional elements such as socio-demographic variables, perceptions regarding cyber security, prior experiences of breaches, and the utilization of information technology also influence awareness; however, discrepancies are evident, like their impacts (Kovačević et al., 2020).

Although studies have examined cybersecurity awareness in corporate or sectoral settings, few have focused on university students in Malaysia using structured, survey-based methods. This study addresses that gap by providing empirical insights into students' levels of awareness, with particular attention to age-based differences, and by highlighting the need for targeted educational interventions to enhance digital resilience within this vulnerable demographic.

4.0 METHODOLOGY

The current study, "Cybersecurity Awareness Levels in the Digital Age: A Study of University Students," follows the guidance of Wang and Cheng (2020)Wang et al., who assert that a cross-sectional survey design should be the preferred course of action when researchers wish to fulfil the research objective in a limited timeframe. An advantage of this strategy is that it enables a rapid and low-cost assessment of both the outcomes in the subjects of the investigation and the exposures of the subjects. To avoid common method bias, as Chang et al. (2010) pointed out, participants were assured of confidentiality and anonymity to encourage honest responses.

Given the challenges in research that complicate gauging respondents' willingness to respond, Eichhorn (2014) noted that this presents an undesirable situation. The present study employed a five-point Likert Scale to gather data, which classifies salient variables of the study. Within this specific research project, the researcher utilized a five-point Likert Scale to collect data, grouping items of substantial importance. It is important to recognize that using these scales, the lowest point, which is 1, indicates the highest level of dissonance in the respondents' views, the next being two which reflects contrary views, while 3 indicates neutral views. Conversely, a rating of 4 suggests that the respondents agree with the presented view. In contrast, the highest scale level, i.e., 5, indicates that the respondents strongly support or endorse the view being considered. The decision to employ a non-probability sampling strategy was primarily due to the researcher lacking an appropriate sampling frame.

Additionally, there are difficulties in obtaining a sampling frame for students in Malaysian universities. The selected respondents were requested to participate as subjects in this study. However, regarding the G*Power analysis concerning the F-Test: Linear Multiple Regression: Fixed model with R^2 deviation from zero, a recommendation of a sample size of at least 119 was made for this particular study. It should be noted that the researcher was only able to recruit 142 participants for the study and thus did not meet the minimum threshold of 119.

The instrument was adapted from Alqahtani (2022), which was initially developed to assess cybersecurity awareness among university students. To ensure contextual relevance and clarity, the adapted questionnaire underwent a pre-test involving five respondents with similar demographic backgrounds to those in the main sample. This process ensured face validity and consistent interpretation of the items. Minor revisions were made based on their feedback to enhance clarity and formatting.

The survey was administered to participants using the Google Forms data collection method, where respondents completed the survey on an Excel spreadsheet, thereby eliminating any possibility of data errors and ensuring that the data collected was accurate and credible. A reliability analysis was conducted to measure internal consistency after complete data collection. The results showed that the instrument exceeded the standard reliability threshold, with a Cronbach's alpha value above 0.70, indicating acceptable internal consistency of the scale items.

5.0 RESULTS AND FINDING

Table 1: Level of Cybersecurity Awareness

	N	Mean	Std. Deviation
Cybersecurity Awareness	142	4.656	.792
Valid N (listwise)	142		

Table 2: Level of Cybersecurity awareness (age)

Age	Mean	N	Std. Deviation
18-24 years old	4.641	122	.809
25-34 years old	4.604	12	.875
35-44 years old	5.000	5	.000
45-54 years old	4.916	3	.144
Total	4.656	142	.792

An assessment of the overall level of cybersecurity knowledge of university students was carried out using a survey involving 142 respondents. Cybersecurity awareness amongst students can be averaged at 4.656 (SD=0.792), as illustrated in Table 1. Such results indicate a high level of awareness amongst the participants. A university student should know enough about cybersecurity concepts and practices. From the results obtained from this study, it is evidenced that most university students possess a relatively satisfactory level of cybersecurity awareness, Mean=4.656, from their responses. As the data broken down by age shows, rather ‘young’ students, aged 18 to 24 years, demonstrate the same level of awareness as the older cohorts, which suggests that educational initiatives do not neglect this population. However, the differences observed in the 25-34 age group should be studied more closely to explain the reasons for their slightly lower mean score. Great expectations or dreadful possibilities are both connected to the 35-44 age group. This age cohort reached the perfect score on cybersecurity awareness despite the low sample population, which suggests their relative experience or training contributes tremendously to their knowledge. This trend is consistent in the higher age group 45-54, where a reasonable number of respondents demonstrated that their awareness of cybersecurity is also above the general expectations. These findings, in general, demonstrate the necessity of conducting regular cybersecurity awareness and training programs for the university population with different age dimensions.

Considering the general level of awareness among university students, it is a justification for the relevance of continuous and advanced cybersecurity education in academic institutions. Though the results produced encouraging trends, the trends are not conclusive since there is still much to be done especially with the mid and early aged 25 to 34 years gap. They should consider addressing the specificities of different age cohorts to ensure the effective delivery of the programs. In addition, the research also suggests how necessary it is to bring some practical insights into the teaching and learning of some cybersecurity concepts. Garcia and Bongo (2022) state that students who completed ICT courses practice better data protection measures and avoid using unsafe applications. To this end, hands-on training, workshops, and simulations based on present-day cybersecurity threats may reinforce students' practical capabilities and acquired theoretical knowledge. These results are consistent with previous studies by Perkasa and Setiawan (2024), who also found that 86.38% of high school students regard cyber awareness level as 'good.' This demonstrates the respondents' relatively high cyber security awareness. As for the study by Booc et al. (2024), high schoolers in Davao City, Philippines also reported high cybersecurity awareness.

They found a significant positive relationship between cyber security awareness and cyber security action, which means that the increased awareness of the students contributes to their responsible actions within cyberspace. Nonetheless, some research findings contradict this, such as those of Ahmad Badela (2024), who, for his part, revealed diverse levels of effectiveness and knowledge among the Politeknik Mersing students regarding cybersecurity, in that there were more than one strength. However, there were also areas where there was considerable lack of knowledge and practices. However, It is worth noting that opening emails from strange contacts and subscribing to the same password everywhere were quite common. This implies that the general level of cyber awareness among students is low, and there is an imperative need to implement specific educational campaigns to enhance students' understanding of and safe practices in cyberspace.

The study conducted by Verma and Pawar (2024)concentrates on the problem of the level of awareness of college students regarding cybersecurity, noting that this level is rather poor. While the number of internet-using students is relatively high, a significant portion of these students do not know important threats like phishing, malware, or ransomware. In their study, Abdukadir Ahmed et al. (2023) experienced a varying degree of cybersecurity awareness among university students in Mogadishu, with some students showcasing a lack of knowledge on essential issues like phishing or even the strength of their passwords. Specifically, SIMAD and Jamhuriya University students complained that they were victims of virus attacks, whereas SIU students reported that they had issues with weak passwords as well as inappropriate use of social networking sites.

The findings of this study indicate a gap in the level of cybersecurity education provided in most colleges or universities, which calls for improvement. These findings are consistent with previous studies that report generally high cybersecurity awareness among student populations. For instance, Perkasa and Setiawan (2024) found that over 86% of high school students rated their awareness as “good,” while Booc et al. (2024) reported a positive relationship between cybersecurity awareness and responsible online behaviour among students in the Philippines. Similarly, Garcia and Bongo (2022) highlighted that student with prior ICT training tend to practice better digital safety, which may explain the perfect awareness scores among the 35–44 age group in this study.

On the other hand, the slightly lower awareness among the 25–34 age group aligns with Ahmad Badela (2024), who identified gaps in knowledge and inconsistent practices among students at Politeknik Mersing. Contrasting findings from Verma and Pawar (2024), who noted poor awareness among college students, and Abdukadir Ahmed et al. (2023), who found varied awareness levels in Somalia, suggest that institutional, cultural, and digital literacy contexts significantly influence outcomes. These comparisons help position the findings within the broader literature and underscore the importance of context-specific educational interventions to strengthen cybersecurity resilience among university students.

Cybersecurity concepts are well portrayed among various students, yet exposure in practice regarding workshops and simulations is a high prerequisite. In contrast, some studies observe students with quite different levels of cybersecurity awareness some students do not even know the term phishing or malware.

Integrating the perspective of business ethics into cybersecurity awareness is of paramount importance, particularly within the framework of future professionals and digital citizens nurtured by higher education institutions. Cybersecurity transcends mere technical proficiency; it embodies a moral and ethical obligation. University scholars, especially those poised to embark on business, management, or information technology careers, must comprehend that their digital conduct may yield substantial repercussions for others. This encompasses the protection of sensitive information, the respect for digital property, and the avoidance of unethical practices, such as unauthorized access or digital plagiarism. Looking at it through an ethical lens, cybersecurity strategies should reflect the foundations of integrity, accountability, openness, and the protection of individual privacy. Students must be instructed that neglecting to adhere to cybersecurity principles such as sharing passwords, disregarding phishing warnings, or circumventing software licenses not only jeopardizes data security but also signifies ethical shortcomings.

As forthcoming participants in corporate or public entities, their ethical posture in digital realms will unequivocally influence organizational trust and societal safety. Incorporating business ethics into cybersecurity education can bolster a culture of ethical digital citizenship. For instance, simulations or workshops may amalgamate case studies wherein students scrutinize cybersecurity dilemmas through ethical paradigms (e.g., utilitarianism versus deontology), thereby enhancing their moral reasoning. As a facet of corporate social responsibility (CSR), contemporary enterprises are anticipated to ensure that their workforce comprehends and adheres to ethical standards in cyberspace; thus, early exposure to this in academic environments equips students for ethically accountable professional behaviour. Consequently, this study emphasizes the significance of cybersecurity awareness at a technical level and underscores the escalating necessity to integrate ethical decision-making into educational methodologies.

6.0 CONCLUSION AND RECOMMENDATION

The current investigation adds to the burgeoning corpus of scholarly work concerning cybersecurity awareness among tertiary education students, particularly within the Malaysian framework. This research elucidates significant perspectives regarding university students' comprehension, attitudes, and behaviours about cybersecurity matters. However, it is crucial to recognize specific limitations that may influence the extent and universality of the results obtained. A predominant limitation is the relatively modest sample size encompassing 142 participants.

Although this sample generated noteworthy initial findings, it introduces constraints requiring further examination, especially about the wider Malaysian student demographic.

Despite the significance and contemporaneity of the study, the comparatively limited sample size restricts its external validity. The demographic composition of university student populations in Malaysia is characterized by considerable diversity, encompassing various geographical regions, cultural backgrounds, academic fields, and digital experiences. While informative, the inclusion of 142 students may not adequately represent this extensive diversity. Consequently, the extrapolation of the study's results to the broader Malaysian student demographic should be undertaken with circumspection.

A small sample size intrinsically constrains statistical power and heightens the probability of sampling error. Furthermore, in the absence of a more extensive cohort of students drawn from a diverse array of universities or regions within Malaysia, the findings may mirror localized trends that fail to encapsulate national patterns. Variations in institutional policies, the availability of digital infrastructure, and cybersecurity measures across universities may also significantly impact students' awareness and behaviours.

The research examined two pivotal demographic variables, age and gender, which yielded valuable insights into the potential variances in cybersecurity awareness across these classifications. This represents a significant strength, as age and gender can substantially affect students' digital literacy, susceptibility to cyber threats, and participation in security practices. For example, younger students may exhibit heightened technological proficiency yet simultaneously engage in more hazardous online behaviours, while older students may exercise greater caution but have diminished exposure to novel digital tools.

Nevertheless, the demographic breadth of the research is constrained in several additional dimensions. Crucial variables such as academic discipline, academic year, prior cybersecurity education, and socioeconomic status were not investigated. These elements are likely to influence students' comprehension and reactions to cybersecurity challenges. As a case in point, students engaged in information technology or engineering programs may display enhanced technical abilities relative to their associates in the arts or social sciences. Likewise, first-year students may demonstrate differing levels of awareness relative to final-year students due to the accumulation of academic experience.

The investigation was executed within a particular institutional framework in Malaysia, presenting an additional contextual limitation dimension. Although such a concentrated methodology facilitates an in-depth examination within a specified environment, it simultaneously constrains the generalizability of the results. Institutional disparities such as divergences in cybersecurity curricula, faculty priorities regarding digital ethics, and the availability of digital literacy resources can significantly affect students' awareness. As a result, the trends identified in this research may not be universally relevant to students attending various Malaysian universities, particularly those situated in rural or less digitally integrated locales.

Moreover, the self-selection nature of the survey participants may have engendered bias. Students with a heightened awareness or interest in cybersecurity might have been more predisposed to engage, potentially distorting the findings toward a more knowledgeable demographic. This phenomenon could lead to overrepresenting general awareness levels among the typical student populace.

In order to enhance the groundwork established by the present investigation and mitigate its shortcomings, several significant avenues for subsequent inquiry are suggested. Expand the Sample Size and Diversity.

Future research endeavours ought to strive for the incorporation of a considerably larger and more heterogeneous sample size that encompasses students from various higher education institutions throughout Malaysia. This approach would facilitate more precise and significant generalizations. Expanding the sample size would augment the reliability of statistical analyses and aid in the discernment of intricate trends across different subgroups.

To promote equitable representation within diverse student cohorts, it is proposed that researchers use stratified sampling techniques founded on vital demographic criteria, such as discipline, year of study, gender, and geographical area. This approach would enable comparative analyses of subgroups and enhance the depiction of disparities in awareness and behavioral patterns across different populations.

In addition to demographic variables such as age and gender, forthcoming research endeavours ought to amass comprehensive data regarding students' academic histories, patterns of digital engagement, prior encounters with cybersecurity education, socioeconomic standing, and the distinctions between urban and rural upbringing. These elements are indispensable for elucidating the intricate dynamics of cybersecurity awareness within Malaysia's multicultural and socioeconomically heterogeneous student population.

In order to monitor variations in awareness across temporal dimensions and evaluate the efficacy of interventions in cybersecurity education, the implementation of longitudinal studies is recommended. Such studies would yield valuable insights into how students' knowledge and practices are enhanced after participating in designated programs, seminars, or curricular modifications. This aspect is particularly critical as digital threats are subject to evolution, necessitating an ongoing refinement of skills.

While this investigation predominantly employed quantitative methodologies, subsequent inquiries would be enhanced by the adoption of a mixed-methodological framework. Incorporating qualitative aspects like interviews or group discussions can shed light on a deeper understanding of how students view, are motivated by, and experience cybersecurity. This methodology would augment the comprehension of the mechanisms underpinning the persistence of certain misconceptions or behaviors, notwithstanding the educational interventions implemented.

Ultimately, forthcoming scholarly inquiries ought to facilitate formulating and assessing pragmatic strategies designed to augment cybersecurity consciousness. This encompasses instructional components integrated within academic curricula, training predicated on simulation methodologies, workshops, or awareness initiatives leveraging digital platforms. We could look at evaluations done before and after, behavioral assessments, or consistent monitoring over time to measure how well these strategies work.

This study offers valuable perspectives regarding the domain of cybersecurity awareness among tertiary education students in Malaysia; nonetheless, it is not without its intrinsic limitations. The constrained sample size, although adequate for preliminary investigation, restricts the capacity to extrapolate findings to the larger populace. While the incorporation of age and gender into the analytical framework enhances the study's depth, the absence of broader demographic and institutional diversity further constrains the interpretive scope. In future inquiries, scholars ought to embark on more inclusive, diverse, and methodologically robust investigations to comprehensively understand the intricate nature of cybersecurity awareness. By undertaking such endeavours, the academic community can furnish evidence-based recommendations that inform curriculum design, institutional policies, and national digital literacy initiatives, thereby ensuring that Malaysian students are adequately equipped to confront the complexities of an increasingly intricate digital landscape.

Author Contribution

Mohd Fazzly Rassis Md Kasim, Wan Hashridz Rizal Wan Abu Bakar, Zuraini Mohamad @ Abdul Rahman, Zarina Kamarozaman jointly contributed to all components of the writing process. Their involvement included developing the introduction, discussing and organizing key ideas, reviewing and refining the language and writing style, as well as editing and preparing the final manuscript draft. All authors collaborated throughout the process and approved the final version of the article.

Conflict of Interest

This manuscript has not been published elsewhere, and all authors have agreed to its submission and declare no conflict of interest regarding the manuscript.

REFERENCES

Alden, D. L., & Hoyer, W. D. (1993). An examination of cognitive factors related to humorousness in television advertising. *Journal of Advertising*, *22*(2), 29–37.

Arif, I., Aslam, W., & Siddiqui, H. (2020). Understanding Consumer Interaction on Instagram: The Role of Satisfaction, Hedonism, and Content Characteristics. *International Journal of Electronic Business*, *15*(2), 109–132.

Casaló, L. V, Flavián, C., & Ibáñez-Sánchez, S. (2017). Understanding consumer interaction on Instagram: The role of satisfaction, hedonism, and content characteristics. *Cyberpsychology, Behavior, and Social Networking*, *20*(6), 369–375.

Casaló, L. V, Flavián, C., & Ibáñez-Sánchez, S. (2020). Influencers on Instagram: Antecedents and consequences of opinion leadership. *Journal of Business Research*, *117*, 510–519.

Daud, M., & Rasiah, R. (2023). Addressing Cybersecurity Issues. In *Digitalization and Development: Ecosystem for Promoting Industrial Revolution 4.0 Technologies in Malaysia*. https://doi.org/10.4324/9781003367093-14

Derbaix, C., & Vanhamme, J. (2003). Inducing word-of-mouth by eliciting surprise–a pilot investigation. *Journal of Economic Psychology*, *24*(1), 99–116.

Dhar, R., & Wertenbroch, K. (2000). Consumer choice between hedonic and utilitarian goods. *Journal of Marketing Research*, *37*(1), 60–71.

Flaherty, K., Weinberger, M. G., & Gulas, C. S. (2004). The impact of perceived humor, product type, and humor style in radio advertising. *Journal of Current Issues & Research in Advertising*, *26*(1), 25–36.

Huffaker, D. (2010). Dimensions of leadership and social influence in online communities. *Human Communication Research*, *36*(4), 593–617.

Jia, Q., Xu, X., Zhou, M., Liu, H., & Chang, F. (2023). Exploring the determinants of continuous intention in TikTok from the perspective of social influence: a mixed approach of SEM and fsQCA. *Journal of Electronic Business & Digital Economics*.

Johari, R. J., Rosnidah, I., & Saaid, N. F. M. (2022). Cybercrime fraud: Malaysian perspective. In *Acceleration of Digital Innovation & Technology towards Society 5.0*. https://doi.org/10.1201/9781003222927-42

Leal, G. P. A., Hor-Meyll, L. F., & de Paula Pessôa, L. A. G. (2014). Influence of virtual communities in purchasing decisions: The participants' perspective. *Journal of Business Research*, *67*(5), 882–890.

Lee, M. T., & Theokary, C. (2021). The superstar social media influencer: Exploiting linguistic style and emotional contagion over content? *Journal of Business Research*, *132*, 860–871.

Mendola, M. A. (2014). *Blogging in the fashion industry: A descriptive study of the use of the two-step flow communications theory by professional and citizen bloggers to become opinion leaders*.

Ning, Y., Hu, C., Tu, T., & Li, D. (2022). Offensive or amusing? The study on the influence of brand-to-brand teasing on consumer engagement behavioral intention based on social media. *Frontiers in Psychology*, *13*, 966254.

Omar, B., & Dequan, W. (2020). *Watch, share or create: The influence of personality traits and user motivation on TikTok mobile video usage*.

Tan, O. S. L., Vergara, R. G., Phan, R. C. W., Khan, S., & Khan, N. (2020). Cybersecurity Laws in Malaysia. In *Encyclopedia of Criminal Activities and the Deep Web*. https://doi.org/10.4018/978-1-5225-9715-5.ch030

Tsang, A. S. L., & Zhou, N. (2005). Newsgroup participants as opinion leaders and seekers in online and offline communication environments. *Journal of Business Research*, *58*(9), 1186–1193.

Wang, Y. (2020). Humor and camera view on mobile short-form video apps influence user experience and technology-adoption intent, an example of TikTok (DouYin). *Computers in Human Behavior*, *110*, 106373.

Weinberger, M. G., Spotts, H., Campbell, L., & Parsons, A. L. (1995). The use and effect of humor in different advertising media. *Journal of Advertising Research*, *35*(3), 44–57.