Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Measuring Cyber Awareness at Don Mariano Marcos Memorial State University

Jonathan J. Estilong[1], Thelma D. Palaoag[2]

[1]College of Computer Science, Don Mariano Marcos Memorial State University, Philippines
[2]College of Computer Science, University of Cordilleras, Baguio City, Philippines
Email: jestilong@dmmmsu.edu.ph

The rise of the Internet, combined with the proliferation of various online applications and consistent engagement with social platforms, has exposed individuals to an assortment of cyber risks. These challenges originating from the global digital connectivity landscape are evident in both professional and educational contexts. Hence, the core objective of this study was to assess the extent of cyber awareness among students and staff at Don Mariano Marcos Memorial State University, particularly focusing on the spheres of cyber safety, cyber security, and cyber privacy. The investigation involved 517 participants who conscientiously completed the Cyber4Dev-Q questionnaire distributed via a Google Form. The results highlighted that although a considerable portion of respondents demonstrated familiarity with cyber security, their comprehension of cyber safety and privacy aspects remained relatively limited. Despite their acknowledgment of diverse cyber risks, the study underscored a palpable deficiency in their grasp of effective strategies to counter cyber-attacks. Furthermore, the research brought to light a significant correlation between cyber awareness and respondents' gender and educational background. Conversely, no substantial link was established between age and status. Overall, the outcomes underscored a disconcerting trend: a majority of respondents showed vulnerability to risks due to their relatively inadequate levels of cyber awareness.

Keywords: cyber awareness, Cyber4Dev-Q, privacy, safety, security.

1. Introduction

The constant evolution of technology propelled by the Internet has fueled an upsurge in online activities spanning academia, government, and industry, yielding global reach. This technological spread has seeped into daily life, touching diverse realms through computers, digital apps, and mobile devices. Heightened convenience and surging demand for online access have catalyzed the widespread embrace of the Internet, commonly known as cyberspace. This trend empowers people to engage in communication, transactions, information retrieval, and social interactions. Nonetheless, this hearty Internet adoption juxtaposes an evident gap in comprehensive awareness concerning diverse cyber threats and attacks. This disparity leaves many individuals ill-equipped to shield their personal data, finances, and devices from potential harm, underscoring the need for fortified protective measures.

Currently, a significant user base of 3.9 billion people, equivalent to nearly half of the world's population, actively engages in the digital landscape, endowing cyberspace with a remarkably pervasive global influence. This prevalence extends across various domains, encompassing educational institutions. As students and educators heavily rely on cyberspace for learning and teaching, they become especially vulnerable to cyber threats [1], [2]. This susceptibility emerges due to a general lack of awareness regarding the potential harm posed by cyber issues within their educational settings. Regrettably, only a handful of studies have undertaken comprehensive investigations to fathom the full scope of these impacts. In this regard, educational institutions emerge as crucial platforms where both students and educators can gain essential insights into cyber safety, security, and privacy. Armed with this knowledge, they can adeptly navigate the intricacies of the digital realm, ensuring their safety and well-being.

As stated by [3], cyber safety encompasses the responsible and secure utilization of information and communication technologies, which includes safeguarding against unwanted marketing and advertising efforts. It involves learning the positive and negative aspects of Information and Communication Technology, attempting to make contact or have a conversation with students online, protecting against cyber intruders, and organizing unsupervised face-to-face meetings with them [4]. Furthermore, cyber safety educates students as well as teachers on cyber ethics (also known as Internet ethics or computer ethics) to use cyber technologies sensibly and responsibly.

Cyber security, on the other hand, is defined as the systematic arrangement of resources, procedures, and frameworks employed to safeguard cyberspace and systems enabled by cyberspace from events that disrupt the alignment between legal and actual property rights. [5]. Its focus is more on the scientific aspects to ensure the safety of users' information in cyberspace. The risk management assurance, best practices, and safeguards [6] are examined under cyber security.

According to [7], privacy is characterized as the assertion of individuals, groups, or institutions to control when, how, and to what degree information about them is disclosed to others. Cyber privacy encompasses both personally identifying information (PII) and non-identifying data, which, when combined, can be utilized to track aspects such as a user's online behavior and cookie-related information.

Insufficient cyber awareness, knowledge, and skills can make individuals vulnerable to cyber risks and threats, including cyberbullying, sexting, and privacy violations, as noted by [8]. The

Cyber Risk Literacy and Education Index reveals that in certain countries, citizens have limited cyber risk literacy, and some nations do not adequately emphasize or assess their cyber risk education requirements. Developing countries confront a distinct set of cybersecurity challenges, characterized by low public awareness of cybersecurity. Many internet users in these regions lack the necessary comprehension and skills to shield themselves from online and mobile security threats, as indicated by [9].

Since the education environment is the area where cyberspace is becoming more prominent, it is essential to note that learners and teachers must be educated on cyber safety, security, and privacy. Schools are mandated to protect learners and teachers and ensure their safety within the educational learning environment. In this light, we perform an assessment on cyber awareness among the students and teachers at the Don Mariano Marcos Memorial State University. This will help university administrators establish a comprehensive training program to avoid or mitigate cyber risks

2. Literature Review

Many researchers have surveyed students and academics to identify cyber safety, cyber security, and cyber privacy awareness.

Researchers [10] delved into the scope and patterns of

problematic internet usage by drawing insights from a cyber awareness initiative carried out in New Delhi. Through this initiative, it was revealed that approximately 19% of the study participants exhibited problematic internet use tendencies. Intriguingly, about 37% of the participants turned to the Internet for mood regulation purposes. The study further identified various factors tied to heightened rates of problematic internet use. These included being male, belonging to older age groups, being enrolled in senior grades, and owning personal digital devices. The specific purposes for internet usage were also found to influence problematic tendencies. Engaging with social media, online gaming, and casual web browsing were positively associated with problematic internet use. In contrast, utilizing the internet for educational activities correlated with lower instances of problems.

Similarly, [11] found that loneliness strongly predicts problematic internet use among university students in Bangladesh, with younger students being more vulnerable. Male students are also more inclined towards problematic internet use. These insights are relevant for university administrators, suggesting the need for educational initiatives to promote a healthy online relationship among students.

Shifting focus to South Africa, [12] undertook an inquiry into the state of cyber safety maturity within schools. The outcomes of this study pointed towards a prevailing deficiency in cyber safety maturity across key components in both private and public schools. The analysis drew attention to education as a particularly underdeveloped facet in this context. The study underscored the need for concerted efforts from government bodies and school management to prioritize and emphasize education for the cultivation of a cyber safety culture within South African schools.

In a study by [13] in the Kyrgyz Republic involving 172 participants, it was found that students were generally unfamiliar with cybercrime. In Northeastern Nigeria, another study [14] assessed students' cybersecurity awareness and found that they had moderate awareness of cyberbullying, self-protection, and internet addiction, with most students having limited basic knowledge of cybersecurity, and female students being more likely to experience cyber victimization. Additionally, a study in Malaysia [15] revealed that one-third of 295 participants had been victims of scams on social networking sites.

Moreover, in a survey at a US Pacific Northwest University with 498 student respondents, 55% were unfamiliar with terms like "Trojan horses," 50% with "phishing," and 17% with "worms" [16], highlighting the need for improved cybersecurity education. Similarly, in Tamil Nadu, India, among 500 participants, 70% were aware of basic virus attacks but 11% used outdated anti-virus software, and over 97% relied on freely available online anti-virus programs, potentially exposing them to malware risks [17].

3. Case and Methodology

Using convenience sampling, the study obtained a sample of employees (faculty and staff) and students at the three campuses of the Don Mariano Marcos Memorial State University (e.g., South La Union Campus, Mid-La Union Campus, and North La Union Campus). The university has a total of 1,433 faculty, 912 staff, and 10,356 students. The link to the questionnaire was distributed online from July 4 to July 18, 2022, due to the physical and social distancing observance catalyzed by the COVID-19 pandemic. A total of 530 responses were returned, and 13 responses were deleted after filtering the completed questionnaires (i.e., respondents have missed or left some questions blank). Hence, 517 responses were used for analysis.

We employed the Cyber4Dec-Q questionnaire, a creation of [7]. It comprises three primary sections. The initial segment comprises 24 context-related questions, aiming to discern respondents' device usage, their purposes, information sources for cyber security, and preferred communication methods. The second section incorporates 29 questions that gauge cyber awareness, categorizing them into cyber safety, cyber security, and cyber privacy. Additionally, it addresses challenges to developing countries, prompted by the Philippines' classification as such in 2022, as per the International Statistical Institute. The questionnaire's final section focuses on demographic information, including designation, gender, age, and educational attainment. Each questionnaire includes an introductory letter and consent form, clarifying the research's intent, ensuring anonymity, emphasizing voluntary participation, and granting the option to withdraw. We designed the questionnaire using Google Forms and distributed it via diverse platforms such as university email, messenger services, and SMS. Participants were estimated to complete it in 15-20 minutes.

Table 1 Hypothesis of the Research Problem

Condition	Decision
P-Value ≥ 0.05	Accept the null hypothesis
P-Value ≤ 0.05	Reject the null hypothesis

Data Analysis

The statistical analysis was performed using SPSS version 21. Descriptive analysis was carried out for demographic, context questions, and cyber awareness outcome variables (e.g., cyber safety, cyber security, and cyber privacy). In the analysis, the frequency and percentage values were calculated. We also measured the answers on cyber awareness on a Likert scale that ranged from 1 – strongly disagree to 5 – strongly agree. We also used the SPSS tool to determine the relationship of the respondents' responses to cyber awareness in terms of gender, age, status, and educational attainment. As shown below, the hypotheses of the research problem, if accepted or rejected, were based on Table 1.

- Hypothesis 1: Is there a significant relationship between gender and cyber awareness?

- Hypothesis 2: Is there a significant relationship between age and cyber awareness?

- Hypothesis 3: Is there a significant relationship between status and cyber awareness?

- Hypothesis 4: Is there a significant relationship between educational attainment and cyber awareness?

4. Result and Discussion

After collecting data, we analyzed the responses or feedback of the 517 respondents from the Don Mariano Marcos Memorial State University on the survey questionnaire. This primarily delves into cyber awareness, focusing on cyber safety, security, and privacy. To achieve this main objective, we analyzed the demographic profile of the respondents as summarized in Table 2.

Table 2 Demographic Information of Research Respondents

Status	N	% of total	Sex	N	% of total
Faculty	98	21.40	Male	152	33.19
Staff	49	10.70	Female	356	77.73
Students	311	67.99			
Age	N	% of total	Highest Educational Attainment	N	% of total
16-25	342	74.67	Highschool	311	67.90
26-36	83	18.12	Bachelor's Degree	86	18.78
Above 36	33	7.20	Technical/Vocational	4	0.87
			Master's Degree	41	8.95
			Doctorate Degree	16	3.49

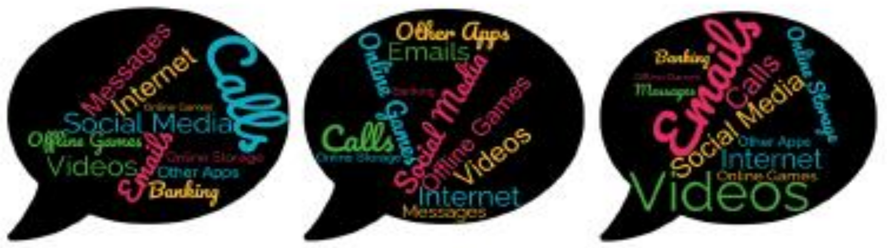
Demographic attributes encompassing employment status, gender, age, and educational achievement were meticulously examined. Evidently, a predominant proportion of the surveyed cohort (67.90%) comprised students, with 21.40% being affiliated with the faculty and 10.70% with the staff. This distribution suggests that students had a comparatively more conducive timeframe for completing the survey. Conversely, the diminished participation from the faculty and staff categories can be ascribed to their pronounced professional commitments during the survey period. The delineation of respondents' roles notably aligns with their age classifications. Specifically, the student demographic, which constitutes a substantial segment

of the overall populace, primarily falls within the 16-25 age bracket (74.67%). In contrast, the faculty and staff strata are distributed across the 26-35 (18.12%) and above 36 (7.20%) ranges, respectively. This empirical outcome substantiates the assertion posited by [19] that students display heightened enthusiasm towards fostering cybersecurity awareness. Moreover, a notable gender-based disparity emerged within the respondent pool, with female participants constituting a larger share (approximately 77.73%) compared to their male counterparts (approximately 33.19%). This observation signifies a heightened inclination among females to actively engage in cybersecurity awareness surveys or learning initiatives, juxtaposed against their male counterparts. As a corollary, it can be posited with a degree of certainty that males might emerge as more susceptible targets of fundamental cyber assaults. Lastly, the predominant segment of respondents reported High School as their highest educational achievement (roughly 67.90%), whereas the remaining participants indicated possession of bachelor's degrees (approximately 18.78%), master's degrees (approximately 8.95%), doctorate degrees (approximately 3.49%), and technical/vocational qualifications (approximately 0.87%).

Evidently, the prevailing status of being college students with a High School level of educational attainment underscores their current unemployed standing, subsequently suggesting a dearth in their exposure to cyber awareness training and education. In light of the escalating incidence of cyber-attacks, the assertion made by [22] gains substantiation, affirming the necessity for high school students to be already well-versed in the intricacies of cybersecurity matters. Cumulatively, the demographic assessment delineates the prevailing profile of respondents as predominantly aligned with Generation Z, encompassing individuals born from 2000 onward to the present day. Relative to the devices used regularly, most of the\ respondents used smartphones (98.40%), followed by those who used desktop computers (54.10%) and tablets/laptops (10.70%). Only a few of them have no devices at all.

As to content question results, Figure 1 exhibits the activities respondents selected for using their smartphones, tablets/laptops, and home/desktop computers. Most of them used their smartphones for phone calls (93.9%), followed by accessing the Internet and sending and receiving emails, with the same percentage of 89.80%. Respondents also access social media (87.00%) such as Facebook, Twitter, etc., and watch videos (84.50%) using their phones. A number of them used their smartphones to send messages (67.80%), play games (54.20%), access some applications (40.90%), save information in the cloud (36%), and 25.90% used their phones to conduct financial transactions via internet banking (25.9%). As depicted in Table 3, a noticeable trend emerges wherein not all survey respondents possessed access to tablet/laptop or home/desktop computer resources. However, among those who owned such devices (10.70% tablet/laptop and 54.10% desktop computer), these tools were primarily utilized for tasks encom passing electronic correspondence, telephony, video consumption, and Internet navigation.

Figure 1 Word Cloud with the Usage of Devices



(a) Cell phone usage (b) Tablet/Laptop usage (c) Home computer usage

Table 3 Devices Used by the Respondents

Device	N	% of total
Smartphones	506	98.40
Tablet/Laptop	55	10.70
Desktop Computer	275	54.10

The outcomes gleaned from this analysis distinctly illuminate the multifaceted engagement of respondents in an array of virtual activities, consequently exposing them to cyberassociated vulnerabilities. Particularly pertinent is the issue of device security, with 87.70% of respondents acknowledging prior instances of smartphone theft, and 10.90% and 7.20% indicating theft occurrences involving their desktop computers and tablets, respectively.

In Figure 2, respondents primarily attribute their cyber knowledge to educational institutions (91.10%), with friends (48.40%) and written resources (31.90%) as secondary sources. An “other” category includes unconventional sources like social media platforms such as Facebook, Twitter, and TikTok, highlighting their influence on cyber awareness among the surveyed cohort.

In Figure 3, most respondents (76.10%) prefer the Internet for future cyber communication, followed by in-person dialogues (62.30%) and SMS (54.40%). The high preference for Internet-based communication among respondents suggests the need for cyber awareness programs to utilize online channels effectively, while also recognizing the continued value of in-person interactions and SMS-based outreach.

Cyber safety

A predominant share of participants exhibited an awareness regarding the susceptibility to stalking (48%) or bullying (44%) threats. Additionally, nearly half (48%) acknowledged personal encounters with unsolicited sexting, while 43% reporting or cyberbullying episodes (57%). Notably, only a modest proportion (26%) of community members demonstrated familiarity with the procedures and resources for reporting cyber linked incidents or transgressions. Furthermore, a substantial 64% of respondents indicated an absence of personal experiences as victims of such cyber offenses. This could potentially stem from a lack of recognition or awareness concerning their exposure to these forms of attacks, thereby rendering them oblivious to their own involvement in such incidents.

Figure 2 Source of Knowledge on Cyber Topics

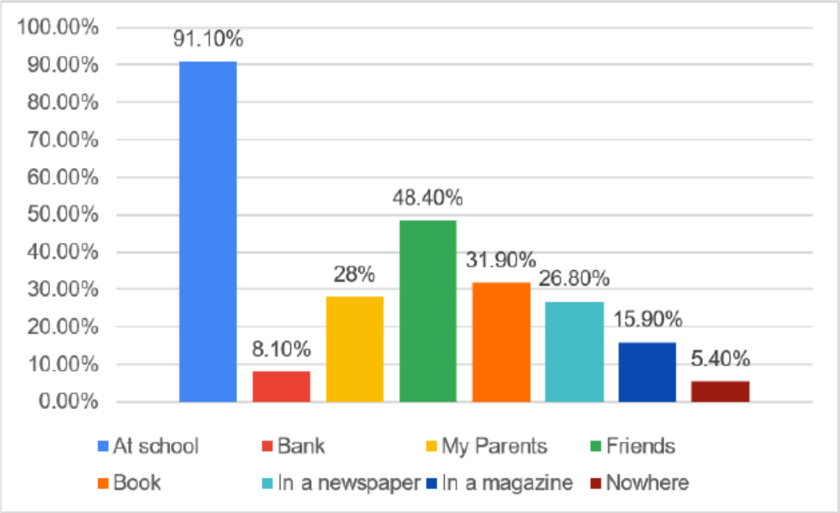
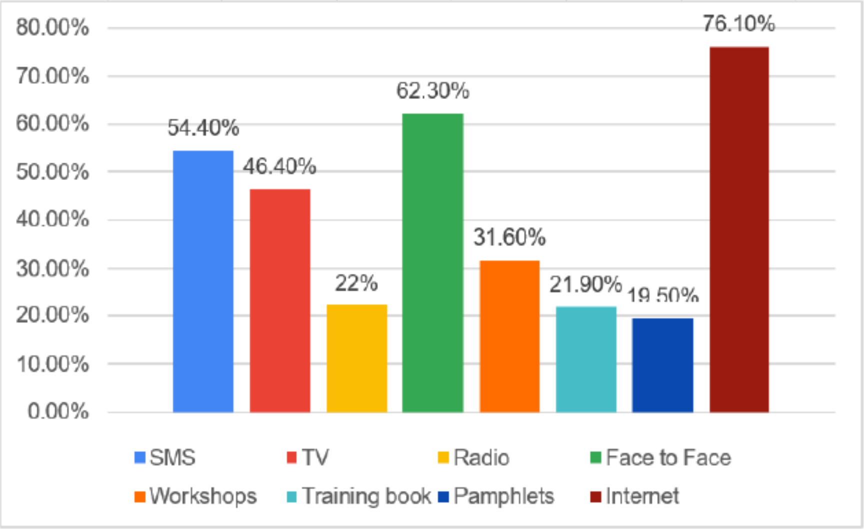


Figure 3 Preferred Method to Learn Cyber Topics



Cyber security

A notable 50% of respondents conveyed their practice of refraining from disclosing personal information to online gaming platforms. This observation suggests a general awareness of the imperative to safeguard personal information. Concurrently, a considerable portion (52%) displayed a proactive stance by choosing not to engage with unsolicited communication or messages from unfamiliar individuals. Furthermore, an appreciable 54% exhibited restraint by abstaining from sharing details concerning their friends or family members in online contexts.

Moreover, a substantial percentage of respondents, numbering 80%, recognized the significance of maintaining backups for their digital data. This trend extends to their comprehension of the potential risks associated with furnishing personal information in response to emails from unknown sources (84%), indicating a commendable understanding of information security risks. The outcomes also highlighted respondents' attentiveness to access control measures. A considerable majority (75%) affirmed their utilization of passwords across their devices, often encompassing a mix of upper and lower case characters, special symbols, and numbers (60%). Additionally, a notable awareness of antivirus software was evident, as 69% acknowledged their familiarity with such tools. However, the deployment of antivirus software was less widespread, with only 46% having it installed on their devices. From a physical security standpoint, the availability of secure locations to safeguard electronic devices was confirmed by 52% of respondents. This observation underscores the salience of the challenges faced by low-income citizens in developing nations, thereby underscoring the real-world implications stemming from the interplay of socio-economic factors and cybersecurity practices. Furthermore, the findings underscore the prevailing cognizance among respondents regarding the susceptibility of their devices to viral infections (90%), the potential infiltration of their devices by malicious actors (74%), and the prospect of their devices being unwittingly involved in cybercriminal activities (78%). This implies that precautions have been taken by the respondents.

Cyber privacy

In the context of cyber privacy, a subset of participants demonstrated an awareness regarding the potential theft of their personal information (46%) or identity (48%) through online channels. However, a prevailing lack of familiarity with website privacy policies was evident, with a mere 38% of respondents knowledgeable about their location. Similarly, the ability to modify default privacy settings was familiar to only 50%, and a comparable 48% claimed comprehension of privacy policies. Interestingly, a perception emerged among respondents that their activities within the digital realm were secure as long as they maintained anonymity or utilized pseudonyms (50%). This sentiment, while common, raises concerns from a cybersecurity and forensic standpoint, given that end users' identities can often be linked to their Internet Protocol (IP) addresses, unless the use of a Virtual Private Network (VPN) is employed. Furthermore, the perspective regarding cyber safety and integrity emerged as intriguing, with merely 42% of respondents deeming the posting or sharing of inaccurate or erroneous information online as unacceptable. This dimension highlights potential misconceptions regarding the responsible use of digital platforms and the ethical implications tied to the dissemination of information within the virtual domain.

Relationship between cyber awareness and demographic profile

Table 4 presents the outcome of the computed Wilk's Lambda test applied to respondents' responses categorized by gender. Examination of the table yields an F statistic of 5.488, accompanied by a probability value of 0.000. Given that the calculated p-value falls below the established margin of error 0.05, the null hypothesis is logically discarded. This inference denotes the presence of a significant association concerning cyber awareness with respect to gender.

Table 4 Gender

Demographics Profile	F	p-value
Gender	5.488	0.000
Age	1.362	0.0101
Status	1.008	0.970
Educ Attainment	1.712	0.007

Delving further into the results, it becomes apparent that the responses from female participants exhibit a substantial correlation with the responses of their female counterparts. This finding coincides with the insights of [20], which suggest that female users possess heightened awareness in contrast to male users, albeit potentially being more vulnerable to diverse threats.

The Wilk's Lambda test for age yielded an F-value of 1.362 with a p-value of 0.101, accepting the null hypothesis. This suggests no significant relationship between cyber awareness and age grouping. This contradicts [21]'s dissertation, which found age to have a significant effect on privacy or security. Table IV also shows the computed Wilk's Lambda test

on the respondents' responses along status. As shown in the table, the F value is 1.008, and the probability value is 0.970. Hence, the null hypothesis is accepted since the p-value is more significant than the 0.05 margin of error. It suggests that there is no significant association with cyber awareness knowledge when grouped based on the respondents' status.

Furthermore, the results of a Wilk's Lambda test on participant responses based on their educational backgrounds are also shown. With an F-value of 1.712 and a p-value of 0.007, the null hypothesis is rejected, indicating a significant link between cyber awareness and respondents' educational categories.

The findings indicate that educational backgrounds have a statistically significant impact on cyber awareness among the participants in this study. This suggests that different levels of education are associated with varying degrees of cyber awareness. Therefore, educational institutions and cybersecurity awareness programs should consider tailoring their efforts to address the specific needs and awareness levels of individuals from different educational backgrounds.

5. Conclusion

Cyber awareness is very important for academic institutions, where most users have no knowledge of the basic concepts of cyber safety, cyber security, and cyber privacy. In this study, we evaluated cyber awareness among employees and students at Don Mariano Marcos Memorial State University, located in La Union, Philippines. The result of this study indicated that most of the respondents are still vulnerable to threats because of their lack of cyber awareness, especially about cyber safety and cyber privacy. Also, it shows that the respondents' responses have a significant relationship to cyber awareness when respondents are grouped as to gender and educational attainment. However, age and status have no significant relationship to cyber awareness. With these, there is really a need to develop a comprehensive strategic plan to disseminate information to people about the necessity of being vigilant in recognizing the most common cyber threat and vulnerabilities. The future work would focus on the conduct of information dissemination through various delivery methods for cyber awareness to fill the missing knowledge identified in this study.

References

1. Kritzinger, E. (2020). Improving cybersafety maturity of South African schools. Information, 11(10), 471.
2. Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. International Journal of Information and Education Technology, 10(5), 378–382.
3. Grey, A. (2011). Cybersafety in early childhood education. Australasian Journal of Early Childhood, 36(2), 77–81.
4. Kwon, M., Seo, Y. S., Nickerson, A. B., Dickerson, S. S., Park, E., & Livingston, J. A. (2020). Sleep quality as a mediator of the relationship between cyber victimization and depression. Journal of Nursing Scholarship, 52(4), 416–425.
5. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10).
6. Dlamini, Z., & Modise, M. (2013). Cybersecurity awareness initiatives in South Africa: A synergy approach. Case Studies in Information Warfare and Security Research Teaching Studies, 1.
7. Da Veiga, A., Loock, M., & Renaud, K. (2022). Cyber4Dev-Q: Calibrating cyber awareness in the developing country context. The Electronic Journal of Information Systems in Developing Countries, 88(1).
8. Peterson, J., & Densley, J. (2017). Cyber violence: What do we know and where do we go from here? Aggression and Violent Behavior, 34, 193–200.
9. Yusif, S., & Hafeez-Baig, A. (2023). Cybersecurity policy compliance in higher education: A theoretical framework. Journal of Applied Security Research, 18(2), 267–288.
10. Balhara, Y. P. S., Harshwardhan, M., Kumar, R., & Singh, S. (2018). Extent and pattern of problematic internet use among school students from Delhi: Findings from the cyber awareness programme. Asian Journal of Psychiatry, 34(3), 8–42.
11. Akhter, M. S., Islam, M. H., & Momen, M. N. (2020). Problematic internet use among university students of Bangladesh: The predictive role of age, gender, and loneliness. Journal of Human Behavior in the Social Environment, 30(8), 1082–1093.
12. Scholtz, D., Kritzinger, E., & Botha, A. (2020). Cyber safety awareness framework for South African schools to enhance cyber safety awareness. In Computer Science On-line Conference (pp. 216–223). Springer, Cham.
13. Ismailova, R., Muhametjanova, G., Medeni, T. D., Medeni, I. T., Soylu, D., & Dossymbekuly, O. A. (2019). Cybercrime risk awareness rate among students in Central Asia: A comparative study in Kyrgyzstan and Kazakhstan. Information Security Journal: A Global Perspective, 28(4-5), 127–135.
14. Garba, A. A., Siraj, M. M., & Othman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern university students in Nigeria. International Journal of Electrical and Computer Engineering (IJECE), 12(1), 572–584.

15. Kirwan, G. H., Fullwood, C., & Rooney, B. (2018). Risk factors for social networking site scam victimization among Malaysian students. Cyberpsychology, Behavior, and Social Networking, 21(2), 123–128.
16. Sarathchandra, D., Haltinner, K., & Lichtenberg, N. (2016). College students' cybersecurity risk perceptions, awareness, and practices. In 2016 Cybersecurity Symposium (CYBERSEC) (pp. 68–73).
17. Senthilkumar, K., & Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in Tamil Nadu. In IOP Conference Series: Materials Science and Engineering (Vol. 263, No. 4, p. 042043). IOP Publishing.
18. Alsagri, H. S., & Alaboodi, S. S. (2015). Privacy awareness of online social networking in Saudi Arabia. In International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA).
19. Bhatnagar, N., & Pry, M. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. Information Systems Education Journal, 18(1), 48–58.
20. Albladi, S. M., & Weir, G. R. (2020). Predicting individuals' vulnerability to social engineering in social networks. Cybersecurity, 3(1), 1–19.
21. Aljohani, N., & Bretas, A. (2021). A bi-level model for detecting and correcting parameter cyber-attacks in power system state estimation. Applied Sciences, 11(14), 6540.
22. Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N. L., & Xu, X. (2022). The influence of social education level on cybersecurity awareness and behavior: A comparative study of university students and working graduates. Education and Information Technologies, 1–32.