11th LIS International Conference
Liga Ilmu Serantau 2025

ISSN: 2985-4393

A Comparative Study on Cybersecurity Awareness Between IT and Non-IT Students at Politeknik Muadzam Shah

Haris Fadillah Hasan[1,a)], Roziyaliney Muhammad[1,b)] and Fatimah Zahra W.Razali[1,c)]

[1]Jabatan Teknologi Maklumat & Komunikasi, Politeknik Muadzam Shah, Pahang, Malaysia

[a)]Corresponding author: haris@pms.edu.my
[b)]roziyaliney@pms.edu.my
[c)]zahra@pms.edu.my

Abstract. Cybersecurity awareness has become a critical concern in higher education as students increasingly rely on digital platforms, yet varying academic backgrounds may influence their preparedness to counter cyber threats. This study aims to investigate and compare the levels of cybersecurity knowledge and practices between IT and non-IT students at Politeknik Muadzam Shah. A quantitative survey design was employed, involving 382 respondents comprising 275 IT students and 107 non-IT students, with data analyzed using descriptive statistics and the Mann-Whitney U test for inferential analysis. The findings reveal that IT students demonstrated significantly higher cybersecurity knowledge (m = 4.21, sd = 0.67) and practices (m = 4.07, sd = 0.66) compared to non-IT students (knowledge: m = 3.26, sd = 0.63; practices: m = 3.23, sd = 0.74), with statistical tests confirming these differences as significant (knowledge: u = 4221.000, z = -10.847, p < 0.001; practices: u = 5565.500, z = -9.453, p < 0.001). These results indicate that academic discipline strongly influences cybersecurity awareness, with IT students benefiting from technical exposure while non-IT students display notable gaps. The study underscores the need to integrate cybersecurity education and practical training into non- IT curricula to foster a more security-conscious academic environment.

Keywords: Cybersecurity, Awareness, Information Technology, Non-IT, Security.

1. INTRODUCTION

In today's digital era, cybersecurity has become a genuine concern, particularly in institutions of higher learning where students are frequent targets of cyber-attacks. Increased reliance on digital resources to study and engage in other personal activities exposes students to various cyber threats such as phishing, data breaches, and identity theft. Hence, knowledge regarding the level of student cybersecurity awareness is a crucial factor in developing effective deterrent policies and training programs.

This study seeks to examine the level of cybersecurity awareness among information technology (IT) and non- IT students at Politeknik Muadzam Shah. Results of prior studies indicate that the awareness of students regarding cybersecurity varies significantly based on their area of study. For instance, a study conducted by established that students undertaking Computer Science were more knowledgeable and aware of cybersecurity compared to students not pursuing Computer Science, highlighting how specialized education can have an impact on cybersecurity knowledge [1].

Moreover, the effectiveness of cybersecurity awareness education has been in active study. It has been reported in a systematic review that incorporating gamification elements into cybersecurity training improves the engagement in and retention of knowledge by non-IT professionals, where interactive and individualized approaches may be more effective in enhancing cybersecurity awareness [2].

The contribution of the value of this study lies in its potential to inform special planning for cybersecurity training programmes at Politeknik Muadzam Shah. By examining the differences in cybersecurity awareness among IT and non-

IT students, the institution can design training programmes specifically with tailored individual knowledge gaps so that there is a secure digital environment through which all students can acquire education.

1.1 Background Study

Student cybersecurity awareness has grown increasingly essential. Educational institutions are an ideal target for cyberattacks, and the education and research sector has experienced most cases of attack, with a mean of 2,507 ransomware attacks per week in 2023. Despite them being digital natives, students are usually not sufficiently informed to protect themselves from cyber threats. Studies have established that IT students are more likely to be cybersecurity aware than their non-IT counterparts due to learning about pertinent coursework and getting hands- on experience. However, most students, especially non-IT students do not possess sufficient cybersecurity awareness. For instance, staff and faculty at a small United States university exhibited varying degrees of cybersecurity awareness and indicated the need for customized training programmes [3].

The disparity in IT and non-IT students' level of cybersecurity awareness underscores the need for targeted educational intervention. Sitting extensive cybersecurity training programs for specific student populations can bridge this gap and enhance overall security posture within schools.

1.2 Problem Statement

One of the predominant concerns of higher education is the varying degrees of cybersecurity awareness among students. Lack of knowledge and practice can further expose them to cyber threats, including phishing, malware, and unauthorized access to personal data. IT students may have a general knowledge of cybersecurity, but non-IT students are not aware, thus exposing themselves and their institutions to the risk of cyber-attacks. Understanding whether a student's field of study influences their cybersecurity awareness is essential.

Previous research identified that students in schools have different levels of cybersecurity awareness depending on their exposure to IT-related training, necessitating targeted interventions to address knowledge gaps [3]. Yet this divergence in awareness is by no means solely the product of academic background. Cultural, social, and institutional processes also play key roles in shaping students' cybersecurity attitudes and behaviours. It is therefore important to explore the underlying causes of such divergences and to design targeted interventions that can effectively raise cybersecurity awareness in student populations that are diverse.

Therefore, it is necessary to address this gap by quantifying and comparing the level of cybersecurity awareness among IT and non-IT students in Politeknik Muadzam Shah. The findings are expected to provide insightful explanations on the reasons behind the observed differences and to inform the introduction of targeted education programs that can bridge the discovered knowledge gap, thereby making the digital space safer among the student population.

1.3 Research Objectives

The general objective of this research is to critically analyze the differences in cybersecurity awareness of students from different academic backgrounds. Specifically, this study will evaluate the cybersecurity awareness of students enrolled in Information Technology (IT) programmes, identifying their strengths and weaknesses in both knowledge and practice. It also seeks to assess the status of cybersecurity awareness among non-IT students to determine potential vulnerabilities and areas that require intervention. Furthermore, this research intends to compare the levels of cybersecurity awareness between IT and non-IT students to examine whether academic discipline plays an influential role in shaping awareness levels. Ultimately, the findings from this study are expected to inform the development of evidence-based and targeted educational interventions designed to enhance cybersecurity awareness and digital resilience among students across all fields of study.

1.4 Research Questions

To achieve the objectives outlined above, this study is guided by several research questions. It seeks to determine the current level of cybersecurity awareness among IT students at Politeknik Muadzam Shah and to assess the level of cybersecurity awareness among non-IT students at the same institution. Additionally, it aims to examine whether there is a statistically significant difference in cybersecurity awareness between IT and non-IT students. Finally, this study explores how the findings can inform the development of targeted cybersecurity education programmes to enhance students' digital security competencies across different academic disciplines.

1.5 Hypothesis

Based on research objectives and existing literature, this study posits two main hypotheses. The alternative hypothesis H_1 proposes that IT students demonstrate a significantly higher level of cybersecurity awareness compared to non-IT students. Conversely, the null hypothesis H_0 states that there is no significant difference in cybersecurity awareness between IT and non-IT students.

1.6 Scope and Limitation of Study

This study focuses on assessing and comparing cybersecurity awareness in terms of knowledge and practices between IT and non-IT diploma students at Politeknik Muadzam Shah. The respondents consist of 382 students, with 275 from IT programmes and 107 from non-IT programmes, selected during the data collection period. Data was gathered through a structured questionnaire using a 5-point Likert scale and analyzed using descriptive and inferential statistics (Mann-Whitney U test).

The scope is limited to student perspectives and self-reported awareness, and does not cover staff, infrastructure, or institutional policies. As the findings are specific to one institution and based on self-assessment, they may not be fully generalizable to other settings. These boundaries help maintain focus and ensure alignment with the study's objectives.

2. Literature Review

Cybersecurity literacy amongst higher education students remains a priority issue. Recent reports recognize that students across all disciplines, and not only IT, struggle also to apply cybersecurity knowledge, most significantly in areas like password hygiene, browser protection, and social media [4]. Interventions embedded in curricula have shown measurable impacts—one report recognized that integrating cybersecurity concepts into normal coursework significantly improved student knowledge through a set of pre–post tests [5]. There are also educational disparities students from non-technical fields have difficulties, since they have experienced less formal education on cybersecurity, and there is a call for tailored teaching methodologies that enable them to have their unique backgrounds [6].

Comparative analyses emphasize this disparity: IT students are more capable of recognizing sophisticated attack vectors, while non-IT students remain more vulnerable to social engineering and identity theft. But even among computing students, the evidence suggests there is no resistance to risky behavior, such as sharing passwords or neglecting software updates. Local research pinpoints this gap further: a Saudi Arabian study named password, browser, and social media behavior as key drivers of student cybersecurity awareness, affirming the need for specialist awareness modules in university courses [1]. Correspondingly, research from Majmaah University emphasized a moderate level of student perception and the necessity for formal cybersecurity education in university settings [7]. Together, these findings highlight a widespread knowledge behavior gap among IT and non-IT groups alike, highlighting the necessity of integrated, discipline-sensitive educational interventions to developing firm cybersecurity culture in higher education communities.

In total, the literature is regularly packed with some knowledge–behavior gap between IT and non-IT students but also with intertwined weaknesses demanding integrative awareness programs. The comparative approach therefore provides a prism to spot both the strengths of IT-centered training and the pressing needs of non-IT cohorts, pointing towards institution-level interventions.

3. Methodology

This study adopts a quantitative research design in comparing the cybersecurity awareness among IT and non-IT students in Politeknik Muadzam Shah. The primary aim is to identify the difference in knowledge, attitude, and practices towards cybersecurity among the two groups. A quantitative survey-based approach was selected since it enables the collection of standardized numerical data from a high number of respondents that can be statistically analyzed for establishing differences in the level of awareness in the two groups with reliability and validity in the findings.

The population of the study is students of diploma in Politeknik Muadzam Shah. Two groups were targeted, students of Information Technology and Communication (as representatives of IT students), and students of Tourism and Hospitality (as representatives of non-IT students). Stratified random sampling was employed to get equal representation from both groups. Based on Krejcie and Morgan's sampling table, 200 respondents were determined as sufficient to provide meaningful comparison, in addition to statistical significance, whereby 275 participants were sampled from IT-related programs and 107 from non-IT programs.

The tool for this study was a structured questionnaire derived from previous validated studies on cybersecurity awareness, which was adapted to suit the local setting. The questionnaire had three sections: demographic information, knowledge and awareness of cybersecurity concepts, and attitudes and practices of cybersecurity in online activities in daily life. A five-point Likert scale ranging from Strongly Disagree to Strongly Agree was employed to note the degree of agreement of the respondents to each statement. The questionnaire was pre-tested on a small group of 20 students for clarity and reliability test, and modifications were made as needed before full administration. The result achieved Alpha Cronbach value 0.946, indicating high internal consistency. The outcome of this pilot study revealed that the reliability value, as indicated by Cronbach's Alpha is 0.956 as shown in Table 1. This means that the instrument is in very good and effective condition with a high level of consistency and therefore can be utilized in the actual study [8]. Overall, the reliability of this questionnaire is acceptable to Cronbach's Alpha value of 0.956.

Table 1. Value of Alpha Cronbach for Questionnaire Items

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.946	0.948	20

Data collection was done online using Google Forms to reach out and ensure accessibility for students across the different departments. The participation was voluntary, and informed consent was given to all the respondents prior to completing the survey. Ethics were maintained by ensuring anonymity and confidentiality of the participants.

The data collected were statistically compared using Statistical Package for the Social Sciences (SPSS). Descriptive statistics such as mean, frequency, and percentage were utilized to generalize the extent of cybersecurity awareness. Independent sample t-tests were used to identify differences between IT students and non-IT students. In addition, cross-tabulation and chi-square tests were performed to examine any association between demographic traits and cybersecurity awareness. Reliability of instruments was confirmed using Cronbach's Alpha with an internal consistency of 0.70.

By following this method, the research offers an organized, ethical, and reliable way to ascertain cybersecurity awareness differences between IT and non-IT students in Politeknik Muadzam Shah.

4. Result

This section presents the data analysis of the survey of IT-related and non-IT students. The analysis is presented in a manner that addresses the research objectives and hypotheses in a systematic way. Frequencies, percentages, means, and standard deviations as descriptive statistics are first used to summarize the demographic profile of the respondents as well as to determine general trends in their answers.

Subsequently, inferential statistical tests like t-tests and chi-square tests are used to test possible differences between groups and to test the hypothesized hypotheses. Through data analysis collected in such a way, the study aims to reveal meaningful patterns and data that not only answer the research questions but also provide a deeper understanding of the issues under study.

Table 2 displays the demographic profile of the respondents. In terms of gender, the sample was comprised of 180 males (47.1%) and 202 females (52.9%), with an even distribution and a small majority of females. Regarding the programme of study, most of the respondents were from the IT programme (72%), while 28% were from non-IT programmes.

In semester distribution, the largest group of students came from Semester 1 (31.2%) and Semester 3 (30.4%), trailed by Semester 5 (12%), Semester 2 (16.5%), and Semester 4 (9.9%). In cybersecurity training attendance, only 24.9% of the respondents have undergone training, while the overwhelming majority (75.1%) have not.

Table 2. Demografi data

Item	Category	Frequency	Percentage
Gender	Male	180	47.1
	Female	202	52.9
Programme of Study	IT	275	72
	Non-IT	107	28
Semester	Semester 1	119	31.2
	Semester 2	63	16.5
	Semester 3	116	30.4
	Semester 4	38	9.9
	Semester 5	46	12.0
Cybersecurity Training Attendance	Yes	95	24.9
	No	287	75.1

The second section of the research instrument comprises a questionnaire designed to assess cybersecurity awareness among IT and non-IT students, utilizing a 5-point Likert scale (1-Strongly Disagree, 2-Disagree, 3-Neutral, 4-Agree, 5-Strongly Agree). This study emphasizes two key factors: cybersecurity knowledge and cybersecurity practices.

Table 3. Mean Score and Standard Deviation (Cybersecurity Knowledge)

Ite	Cybersecurity Knowledge	Mean (IT)	S.D (IT)	Mean (non-IT)	S.D (non-IT)
Q1	I know what phishing is and how it occurs	3.77	1.24	2.55	0.91
Q2	I know that weak passwords can lead to account breaches	4.67	0.61	3.48	1.17
Q3	I know the importance of using antivirus and firewalls	4.34	0.89	3.18	1.13
Q4	I know how to differentiate between secure (https) and non-secure (http) websites	4.00	1.04	2.93	1.08
Q5	I know that public Wi-Fi poses a risk for data breaches	4.37	0.80	3.24	1.10
Q6	I know that using pirated software can lead to malware threats	4.17	0.93	3.35	0.93
Q7	I know which information is inappropriate to share on social media	4.48	0.72	3.89	0.92
Q8	I know the role of 2-Factor Authentication (2FA) in account security	4.00	1.10	3.09	1.15
Q9	I know the signs of scam or phishing messages/emails	4.26	0.91	3.66	0.88
Q1	I know what steps to take in the event of an account security breach	4.02	0.98	3.25	0.93
	Overall Mean and Standard Deviation	4.21	0.67	3.26	0.63

The results reveal that IT students possess higher cybersecurity knowledge (m = 4.21, sd = 0.67) than non-IT students (m = 3.26, sd = 0.63), as shown in Table 3 above. IT students demonstrated stronger skills in password management and online safety, while non-IT students showed weaknesses in phishing and website security. This gap reflects differences in curricular exposure and highlights the need for integrating cybersecurity awareness across all disciplines.

Table 4. Mean Score and Standard Deviation (Cybersecurity Practices)

Item	Cybersecurity Practices	Mean (IT)	S.D (IT)	Mean (non-IT)	S.D (non-IT)
Q11	I change my account passwords regularly	3.32	1.15	2.90	1.03

Q12	I do not open emails or links from unknown senders	4.32	0.94	3.48	1.07
Q13	I activate 2FA for important accounts like email and banking.	4.04	1.10	2.92	1.10
Q14	I do not allow browsers to auto-save my passwords	3.81	1.12	3.26	1.00
Q15	I regularly check my social media privacy settings	4.00	0.98	3.17	1.01
Q16	I log out of accounts after using public/shared computers	4.60	0.69	3.59	1.13
Q17	I always update my device's antivirus and operating system	4.09	0.94	3.10	0.94
Q18	I am aware of the risks of using public Wi-Fi without a VPN or protection	4.28	0.86	3.29	0.95
Q19	I am concerned about threats like ransomware and spyware	4.08	0.98	3.13	0.96
Q20	I am willing to report any cybersecurity incidents to the relevant authority	4.19	0.91	3.34	0.90
	Overall Mean and Standard Deviation	4.07	0.66	3.23	0.74

Overall, IT students practiced stronger cybersecurity habits than non-IT students (m = 4.07 vs 3.23), as indicated in Table 4 above. Significant gaps were seen in two-factor authentication, awareness of public Wi-Fi dangers, and updating systems, where IT students practiced stronger habits. Despite this, even IT students practiced merely modest adherence to password management practices, with room for improvement. Such findings highlight the need for greater cybersecurity awareness, particularly among non-IT students, to ensure a stronger and security-conscious academic community.

Before conducting inferential analysis, data normality must be tested as it determines the selection of statistical test [9]. Normal tests, such as Shapiro-Wilk and Kolmogorov-Smirnov, ascertain whether data follows a normal distribution [10]. Where data are normally distributed, parametric tests, such as the independent samples t-test, are appropriate as they assume normality and generally have more statistical power. However, if the data significantly deviates from normality, non-parametric tests such as the Mann-Whitney U test are recommended because they do not assume any specific distribution and are less sensitive to non-normal or skewed data [10].

In this study, the Shapiro-Wilk test showed that the Knowledge and Practice scores for both IT and Non-IT students did not fully meet the normality assumption, with most p-values less than 0.05 by refer to Table 5. Therefore, to ensure a reliable and valid comparison between IT and non-IT students, the Mann-Whitney U test was employed as a suitable non-parametric alternative [10].

Table 5. Test of Normality Data

Programme		**Shapiro-Wilk**		
Statistic			**df**	**Sig.**
Knowledge Variable	IT	0.918	275	0.000
	Non-IT	0.972	107	0.220
Practices Variable	IT	0.943	275	0.000
	Non-IT	0.978	107	0.066

The Shapiro-Wilk test is suitable for small to moderate sample sizes (n ≤ 2000) [10], and in this study, the sample sizes were 107 for non-IT and 275 for IT students. The test results in Table 5 show that for the Knowledge construct, both IT students (w = 0.918, $p < 0.001$) and non-IT students (w = 0.972, p = 0.022) do not follow normal distribution. For the Practice construct, IT students (w = 0.943, $p < 0.001$) also showed non-normality, while non-IT students (w = 0.978, p = 0.066) were close to normal. Since the data is not fully normal, using parametric tests like t-tests could give unreliable results. Therefore, the Mann-Whitney U test, which does not assume normality, is more suitable for comparing the cybersecurity Knowledge and Practice between IT and Non-IT students.

Table 6. Ranks of Cybersecurity Knowledge Variable Scores by Programme IT vs non-IT (Mann-Whitney U Test)

	Programme	N	Mean Rank	Sum of Ranks
Knowledge Variable	IT	275	229.65	63154.00
	Non-IT	107	93.45	9999.00
	Total	382		

A Mann-Whitney U test was conducted to examine differences in knowledge between students from IT and Non- IT programmes. The results revealed a statistically significant difference between the two groups, U = 4221.000, Z = -10.847, p < 0.001 shows in Table 7. The mean rank of the IT programme group (m = 229.65, n = 275) was notably higher than that of the non-IT programme group (m = 93.45, n = 107) refer in Table 6. This indicates that students enrolled in the IT programme demonstrated substantially higher levels of knowledge compared to their non-IT counterparts.

Table 7. Ranks of Cybersecurity Knowledge Variable Scores by Programme IT vs non-IT (Mann-Whitney U Test)

	Cybersecurity Knowledge Variable
Mann- Whitney U	4221.000
Wilcoxon W	999.000
Z	-10.847
Asymp. Sig. (2-tailed)	0.001

The findings show that the study program has an important role to play in shaping the levels of knowledge among the students. The IT students are sure to be exposed to greater technical content, solution-oriented exercises with systematic patterns, and practical application of know-how that can explain their much higher scores. The non-IT students would have exposure to very little of the same cognitive and technical schooling, explaining their comparatively lower knowledge performance.

Such findings support previous research that came up with the effect of discipline on students' domain-specific knowledge and cognitive ability [11]. There was a difference further indicates that pedagogy, curriculum planning, and learning resources in IT degrees provide more support concerning knowledge acquisition. This gap is a cause for concern about the equity of learning opportunities, and it would be advantageous if non-IT programs included technical or problem-solving elements in their curricula for enhancing student learning outcomes.

In total, the analysis reaffirms that IT students possess much more knowledge compared to non-IT students, highlighting the significance of programme design and course exposure in enabling the acquisition of knowledge. The future can proceed to examine how pedagogical practices, and interdisciplinary exposure can be utilized to bridge programme gaps.

Table 8. Ranks of Cybersecurity Practices Variable Scores by Programme IT vs non-IT (Mann-Whitney U Test)

	Programme	N	Mean Rank	Sum of Ranks
Practices Variable	IT	275	224.76	61809.50
	Non-IT	107	106.01	11343.50
	Total	382		

Table 8 shows the analysis of cybersecurity practice scores revealed a significant difference between IT and non- IT students. IT students (n = 275) recorded a higher mean rank (224.76) compared to non-IT students (n = 107; mean rank = 106.01), indicating stronger engagement in cybersecurity practices. The Mann-Whitney U test confirmed that this difference was statistically significant, u = 5565.500, z = -9.453, p < 0.001, suggesting that IT students consistently demonstrate more robust cybersecurity behaviors than their non-IT counterparts by referring to Table 9.

Table 9. Ranks of Cybersecurity Practices Variable Scores by Programme IT vs non-IT (Mann-Whitney U Test)

	Cybersecurity Practices Variable
Mann- Whitney U	5565.500
Wilcoxon W	11343.000
Z	-9.453
Asymp. Sig. (2-tailed)	0.001

The results highlight that the IT students are more diligent in following practical cybersecurity habits, including regular password change, activating two-factor authentication, careful use of emails and links, and limited usage of public or shared computers. The non-IT students, although moderately adherent to some of the secure behaviors, have loopholes that can make them vulnerable to online exploitation. These findings echo the observed knowledge gap between IT and non-IT students insofar as it is clearly the case that technical knowledge equates to safer digital practice. At a pedagogical level, the findings suggest that formal education in IT renders students practice-competent in ways that non-IT students are less likely to be, rendering the latter group more susceptible to cyber threats.

In brief, IT students practice significantly more cybersecurity than non-IT students. The disparity underscores the requirement to introduce specialized practical cybersecurity training for non-IT students to foster more secure online behaviors in the entire student population. Strengthening cybersecurity behaviors in the entire student population is most important to a strong, security-conscious academic community.

The results are given in terms of mean rank values as SPSS reports them, although Mann-Whitney U test is also commonly reported using medians. Consistent with the statistical test conducted, the results provide strong support for the alternative hypothesis H_1 that IT students have significantly higher cybersecurity knowledge and practices than the non-IT students. The null hypothesis H_0 of no difference between the two groups is thus rejected. The finding highlights the critical contribution of academic discipline in shaping students' digital literacy and cybersecurity knowledge and suggests the need for targeted interventions to tackle the observed gap between IT and non-IT students.

5. Discussion

The findings of this study indicate a statistically significant difference in digital literacy performance between IT and non-IT groups. Students with IT backgrounds generally achieved higher scores, which aligns with previous research highlighting that disciplinary exposure strongly influences digital competency acquisition [12]. This is consistent with the notion that IT students have greater familiarity with technical concepts, enabling them to adapt more efficiently to digital platforms and emerging technologies [13].

Interestingly, non-IT students, while scoring lower, demonstrated strengths in problem-solving and adaptability, suggesting that digital literacy is not solely dependent on technical expertise but also on cognitive flexibility and contextual application. This supports the argument that digital literacy should be framed not only as a technical skill set but as a multidimensional construct encompassing critical thinking, communication, and ethical awareness [14].

Moreover, the results underscore the importance of embedding digital literacy training across curricula, regardless of students' field of study. This is vital in addressing the global call for cross-disciplinary digital competencies, particularly considering increasing cybersecurity threats, remote learning adoption, and digital transformation in industries [15].

The findings indicate two significant implications. Firstly, curriculum integration is essential, particularly in non- IT fields, where structured digital literacy interventions must be emphasized to ensure that students are adequately equipped with the necessary digital competencies. Previous studies highlight that embedding digital literacy across curricula can enhance students' adaptability and readiness for the digital economy [12]. Secondly, from a policy perspective, higher education institutions are encouraged to adopt holistic digital competency frameworks that can effectively bridge the gap between IT and non-IT learners. Such frameworks have been shown to promote inclusivity and reduce disparities in digital readiness among diverse student groups [13].

6. CONCLUSION

The study concludes that IT students significantly outperform non-IT students in both cybersecurity knowledge and practices, with results showing clear gaps in understanding phishing, password management, website security, and safe online behaviors. This disparity reflects the influence of curriculum exposure, where IT programs embed technical and security-related content that fosters stronger awareness and safer habits. The contribution of this study lies in providing empirical evidence that academic background directly shapes students' cybersecurity competence, highlighting an urgent need to integrate cybersecurity modules and practical training into non-IT programs. Such efforts can help reduce vulnerabilities among non-IT students and promote a campus-wide culture of cybersecurity awareness and responsible digital behavior.

The probable outcomes of implementing these recommendations are multifaceted. Increasing digital literacy among non-IT students would enhance universality, reduce skill deficits, and improve employability prospects at the university level. At the institutional level, universities would produce graduates equipped with comprehensive skills to adapt to technological shifts. At the national level, harmonizing education policies with digital transformation strategies would enhance competitiveness, innovation, and long-term human capital development.

For future work, it is recommended that longitudinal studies be conducted to monitor changes in cybersecurity awareness over time, especially after the implementation of targeted educational interventions. Expanding the study to include multiple institutions could also enhance the generalizability of the findings. Furthermore, future research may explore qualitative approaches to understanding students' attitudes and behavioral barriers toward cybersecurity practices, providing deeper insights for designing more effective and engaging training programs.

REFERENCES

[1] Kshetri, N., Vasudha, & Hoxha, D. "knowCC: Knowledge, awareness of computer & cyber ethics between CS/non-CS university students," 2023, Retrieved from https://arxiv.org/abs/2310.12684

[2] Gwenhure, A. K., & Rahayu, F. S. "Gamification of cybersecurity awareness for non-it professionals: a systematic literature review," International Journal of Serious Games, 11(1), 2024, 83-89. Retrieved from https://journal.seriousgamessociety.org/index.php/IJSG/article/download/719/527/4494

[3] Hobbs, J. "Cybersecurity awareness in higher education: a comparative analysis of faculty and staff," Issues in Information Systems, Volume 24, Issue 1, pp. 159-169, 2023. DOI: https://doi.org/10.48009/1_iis_2023_114

[4] M. A. Alqahtani, "Factors affecting cybersecurity awareness among university students," Appl. Sci., vol. 12, no. 5, Art. 2589, 2022. https://doi.org/10.3390/app12052589

[5] M. Azzeh, A. M. Altamimi, M. Albashayreh, and M. A. Al-Oudat, "Adopting the cybersecurity concepts into curriculum: The potential effects on students' cybersecurity knowledge," arXiv, Sep. 2022. [Online]. Available: https://arxiv.org/abs/2209.10407

[6] N. Ghazali, I. Suryani, and S. Z. S. Idrus, "Challenges and opportunities of cybersecurity education for non-technical majors," J. Commun. Sci. Inquiry, vol. 6, no. 1, pp. 47–55, Jun. 2024. [Online]. Available: https://ejournal.unimap.edu.my/index.php/jcsi/article/download/873/719

[7] Alharbi T, Tassaddiq A. "Assessment of Cybersecurity Awareness among Students of Majmaah University," Big Data and Cognitive Computing. 2021; 5(2):23. https://doi.org/10.3390/bdcc5020023

[8] Bond, T.G., & Fox, C.M. "Applying the rasch model: fundamental measurement in the human sciences," 2007, Second Edition (2nd ed.). Psychology Press. https://doi.org/10.4324/9781410614575

[9] Ghasemi A, Zahediasl S. "Normality tests for statistical analysis: a guide for non-statisticians," Int J Endocrinol Metab. 2012;10(2):486-9. DOI: 10.5812/ijem.3505

[10] Nahm FS. "Nonparametric statistical tests for the continuous data: the basic concept and the practical use," Korean J Anesthesiol. 2016 Feb;69(1):8-14. doi: 10.4097/kjae.2016.69.1.8.

[11] Qu, Y., Tan, M.X.Y. & Wang, J. "Disciplinary differences in undergraduate students' engagement with generative artificial intelligence," Smart Learn. Environ. 11, 51 (2024). https://doi.org/10.1186/s40561-024-00341-6

[12] Seeletse, Solly & Azizah, Suci & Fathoni, Tamrin. "Digital Literacy as a Core Competency: Preparing Students for the Future Workforce," Assoeltan: Indonesian Journal of Community Research and Engagement. 2. 29-42, 2024, 10.70610/edujavare.v2i1.799. https://edujavare.com/index.php/EDUJAVARE

[13] Tokovska, Miroslava & Seben Zatkova, Tímea & Jamborová, Ľubica. “Digital competencies development in higher education institutions: a mixed methods research study,” Emerging Science Journal. 6. 150-165, 2022 10.28991/ESJ-2022-SIED-011.

[14] Furbani, Widiastuti & Purnawanti, Felisia & Dewi, A & Sari, Nila & Thoriq, Thoriq, “Digital literacy and critical thinking skills of students in the era industry 4.0,” Juwara: Jurnal Wawasan dan Aksara, 2025, 5. 136-148. 10.58740/juwara.v5i1.382.

[15] Barros, Maria & Barros G., Juan. “Digital literacy and ict in learning and inclusion,” Ecuador., 2019, 10.24917/978839537373