International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.
© 2024 Scholar AI LLC.

Vol. 45 No. 1 June 2024, pp. 304-314

Analyzing Student Academic Performance and Cybersecurity Awareness Levels: Basis for Enhancing Instruction

Rhoel Anthony G. Torres[1] and Cris Norman P. Olipas[2]

[1]College of Information and Communications Technology
Nueva Ecija University of Science and Technology
Cabanatuan City, Philippines
ragtorres@gmail.com

[2]College of Information and Communications Technology
Nueva Ecija University of Science and Technology
Cabanatuan City, Philippines
olipas.cris@gmail.com

Abstract— This study examines the academic performance and cybersecurity awareness levels among first-year Information Technology (IT) students enrolled in ITNET-02 (Networking 2) course at the College of Information and Communications Technology, Nueva Ecija University of Science and Technology Sumacab Campus, during the academic year 2023-2024. In a descriptive quantitative research design, the researchers collected data by administering a structured survey questionnaire to 138 respondents. The demographic profile reveals a predominantly male student cohort, with a significant portion reporting prior experience or background in networking or cybersecurity. Academic performance analysis indicates satisfactory achievement levels across various grading categories, reflecting a foundational understanding of IT concepts among the students. In terms of cybersecurity awareness, respondents demonstrate a high level of knowledge of general cybersecurity principles, phishing awareness, safe online practices, cybersecurity behaviors, and incident response. Based on these findings, recommendations for further instructional quality improvement include integrating targeted cybersecurity modules into the curriculum, emphasizing practical applications of cybersecurity principles, fostering a gender-inclusive environment in IT education, and providing ongoing professional development for educators to enhance teaching effectiveness in cybersecurity topics. This study provides valuable insights into the current academic performance and cybersecurity awareness levels among IT students in the research locale, highlighting opportunities for enhancing educational strategies and preparing students to address cybersecurity challenges in their academic and professional endeavors.

Keywords— Academic Performance, Cybersecurity Awareness, Descriptive, Information Technology, Instruction

I. INTRODUCTION

Cybersecurity has emerged as a critical concern in the digital age due to the escalating cyber threats faced by organizations and individuals worldwide. The interconnected nature of the digital world [1] has created a landscape vulnerable to various security vulnerabilities in fields like the Internet of Things, blockchain, government, and finance. The rise in cybercrimes and cyberattacks [2] underscores the pressing need for robust cybersecurity measures to safeguard data and information from malicious actors. The severity and sophistication of cyber threats [3] necessitate investments in cybersecurity solutions, employee education on best practices, and proactive strategies to mitigate risks effectively. In essence, cybersecurity plays a pivotal role in protecting against digital crimes and ensuring the security of sensitive information in today's technology-driven world.

Education is critical in preparing individuals for cybersecurity concerns by increasing their awareness and ability to combat cyber threats effectively. According to studies, human error accounts for 95% of security events, emphasizing the necessity of teaching individuals about cybersecurity dangers and safe online habits [4]. Furthermore, incorporating game-based approaches into teaching has been found to raise students' cybersecurity awareness and motivation in pursuing cybersecurity jobs, proving the efficacy of novel instructional approaches in combating cyber threats [4]. IT education is critical for increasing cybersecurity awareness among students by addressing vulnerabilities caused by technical improvements and online activities [5]. College students, who rely significantly on technology, are especially vulnerable due to a lack of awareness about cybersecurity threats such as phishing and malware assaults [6, 7].

Academic performance in IT courses, particularly in areas such as networking, can significantly impact students' cybersecurity awareness. Research suggests that integrating cybersecurity topics into academic programs enhances students' attitudes and behaviors towards cybersecurity [8]. Furthermore, students stress the importance of specific knowledge in IT protection courses to bridge the gap between cyber knowledge and protective behaviors, indicating that a focused curriculum can substantially improve cybersecurity practices [9]. The lack of awareness of secure coding among undergraduates underscores the need for targeted training and awareness programs within academic settings to address cybersecurity vulnerabilities effectively [10]. By incorporating cybersecurity awareness into IT courses, universities can better equip students with the necessary skills to combat cyber threats and contribute to a more secure digital environment.

Despite the well-documented importance of cybersecurity education and the integration of cybersecurity topics into academic programs, there remains a significant research gap in understanding the current levels of cybersecurity awareness among students and how this awareness can be leveraged to enhance the quality of instruction. While existing studies highlight the benefits of incorporating cybersecurity topics into curricula and the necessity of specific knowledge in IT protection courses, there is limited research on how to effectively utilize student academic performance data to inform instructional strategies aimed at improving cybersecurity education. This study aims to address this gap by analyzing student academic performance and cybersecurity awareness levels, providing a basis for developing targeted educational interventions and curriculum enhancements that better prepare students for the cybersecurity challenges of the digital age.

A. Research Problems

This study seeks to analyze the academic performance of the IT students and their cybersecurity awareness to provide a basis for instructional quality improvement. Specifically, it aims to answer the following research problems

1. How may the demographic profile of the respondents be described in terms of

   1.1. Sex;

   1.2. Age;

   1.3. Prior experience or background in networking or cybersecurity;

2. How may the academic performance in networking course of the IT students be described?

3. How may the level of the cybersecurity awareness be described in terms of

   3.1. General Cybersecurity Knowledge;

   3.2. Awareness of Phishing and Social Engineering;

   3.3. Safe Online Practices;

   3.4. Cybersecurity Behaviors and Attitudes; and

   3.5. Incident Response Awareness?

II. Methodology

The study employed a quantitative research method, using a descriptive design, to examine the levels of academic performance and cybersecurity awareness among information technology students. It was conducted at the College of Information and Communications Technology at the Nueva Ecija University of Science and Technology Sumacab Campus, focusing on first-year students enrolled in the ITNET02: Networking 2 course during the academic year 2023-2024. Respondents were selected through purposive sampling, with criteria that included being in their first year and currently enrolled in the ITNET02 course.

To collect data, the researchers developed a self-made survey questionnaire. The content of this instrument was reviewed by various experts in the field to ensure its validity and reliability. Additionally, the self-made instrument underwent reliability analysis to confirm its consistency. Table 1 presents the results of the reliability analysis of the developed instrument.

TABLE I. RELIABILITY ANALYSIS

Variable	No. of Items	Cronbach’s Alpha	Reliability Level
General Cybersecurity Knowledge	5	0.806	Good
Awareness of Phishing and Social Engineering	5	0.779	Acceptable
Safe Online Practices	5	0.738	Acceptable
Cybersecurity Behaviors and Attitudes	5	0.808	Good
Incident Response Awareness	5	0.884	Good

Data collection was meticulously planned to uphold ethical standards. Informed consent was obtained from all respondents to ensure their voluntary participation, safeguarding their autonomy and willingness to contribute to the study. The data were gathered using a structured survey questionnaire, which was distributed via Google Forms during the second semester of the academic year. This approach facilitated efficient and accessible data collection while maintaining the integrity of the responses.

For data analysis, the researchers employed statistical techniques, specifically mean and percentage distribution, to evaluate the levels of students' academic performance and their cybersecurity awareness. These techniques enabled the researchers to quantify the data and provide a detailed description of the variables under study.

Ethical considerations were rigorously adhered to throughout the research process. The principles of confidentiality and anonymity were strictly maintained, ensuring that respondents' identities and responses were protected. Additionally, the researchers emphasized the importance of informed consent and voluntary participation, ensuring that respondents were fully aware of the study's purpose and their right to withdraw at any time without any repercussions. These ethical measures were integral to maintaining the integrity and credibility of the research.

III. RESULTS AND DISCUSSION

3.1. The Demographic Profile of the Respondents

Understanding the demographic profile of student respondents is essential for contextualizing the analysis of the academic performance and cybersecurity awareness among BSIT students. Demographic factors such as sex and age may influence students' access to resources, prior experiences, and perceptions, which can in turn impact their academic performance and cybersecurity awareness levels. By considering these demographic variables, educators and policymakers can tailor interventions and educational strategies to address the unique needs and challenges of different student groups, ultimately enhancing the effectiveness of efforts to improve cybersecurity awareness and academic performance in BSIT programs.

TABLE II. DISTRIBUTION OF RESPONDENTS BY SEX

Sex	Frequency	Percentage
Male	108	78.3%
Female	30	21.7%
Total	**138**	**100.0%**

Table 2 displays the distribution of respondents by sex. Out of a total of 138 respondents, 108 are male, comprising 78.3% of the sample, while 30 are female, making up 21.7% of the sample. This indicates a significant predominance of male respondents compared to female respondents within the study population. The implications of these results for the study of academic performance and cybersecurity awareness are noteworthy. Given the larger proportion of male respondents, the findings may primarily reflect male students' academic performance and cybersecurity awareness. This gender disparity suggests that the study's conclusions might be more applicable to male students, potentially overlooking gender-specific differences in these areas. Moreover, the predominance of male respondents aligns with the typical gender distribution in Bachelor of Science in Information Technology (BSIT) programs, where male students often outnumber female students. Male students tend to be more dominant than female students in BSIT programs due to various factors. Research indicates that stereotypes and cultural expectations play a significant role in shaping gender disparities in IT fields [11]. Authors [12] expressed that female students face challenges in choosing IT majors, despite performing equally well as male students, leading to a lower likelihood of selecting BSIT program.

To ensure a more balanced understanding of academic performance and cybersecurity awareness across all student demographics, future research should aim for a more equal gender distribution. This would help identify any distinct patterns or needs among female students, contributing to more targeted and effective educational interventions and support programs.

TABLE III. DISTRIBUTION OF RESPONDENTS BY AGE

Age	Frequency	Percentage
18	36	26.1%
19	82	59.4%
20	16	11.6%
21	2	1.4%
22	1	0.7%
24	1	0.7%
Total	**138**	**100.0%**

Table 3 presents the distribution of respondents by age. The majority of respondents, comprising 59.4% of the sample, are 19 years old. The second largest group consists of respondents who are 18 years old, accounting for 26.1% of the sample. There are smaller proportions of respondents in the older age groups, with 20-year-olds representing 11.6% of the sample, 21-year-olds comprising 1.4%, and both 22-year-olds and 24-year-olds each accounting for 0.7% of the sample. These results indicate that the majority of respondents are in the age range typically associated with first-year college students, with a smaller number of older students also participating in the study.

TABLE IV. DISTRIBUTION OF RESPONDENTS BY AGE

Prior Experience or Background in Networking or Cybersecurity	Frequency	Percentage
Yes	74	53.6%
No	64	46.4%
Total	**138**	**100.0%**

Table 4 presents the distribution of respondents based on their prior experience or background in networking or cybersecurity. Among the 138 respondents, 74 individuals, constituting 53.6% of the sample, reported having previous experience or background in networking or cybersecurity. Conversely, 64 respondents, accounting for 46.4% of the sample, indicated no prior experience or background in these fields.

These findings hold significant relevance for the study on Academic Performance and Cybersecurity Awareness of IT Students. Firstly, the prevalence of respondents with prior experience or background in networking or cybersecurity suggests that a considerable portion of the sample may possess a foundational understanding of these concepts. This could potentially influence their academic performance and cybersecurity awareness, as they may have had exposure to relevant topics before entering the academic environment.

Conversely, the presence of respondents with no prior experience or background in networking or cybersecurity highlights a cohort that may require additional support or resources to develop their skills and awareness in these areas. Understanding the needs and challenges faced by these individuals is crucial for educators and policymakers to tailor interventions and educational strategies effectively.

Overall, the distribution of respondents based on their prior experience or background underscores the diversity within the student population and emphasizes the importance of considering individual differences when addressing academic performance and cybersecurity awareness in the IT education domain.

3.2. The Academic Performance of the BSIT Students

TABLE V. DISTRIBUTION OF RESPONDENTS BY ACADEMIC PERFORMANCE IN ITNET-02

Grade	**Frequency**	**Percentage**
1.25	9	6.5%
1.50	39	28.3%
1.75	36	26.1%
2.00	25	18.1%
2.25	17	12.3%
2.50	3	2.2%
2.75	9	6.5
Total	**138**	**100.0%**

Table 5 presents the distribution of respondents by academic performance in the ITNET-02 course. The highest grade achieved by any respondent is 1.25, with 9 respondents achieving this grade, constituting 6.5% of the sample. The majority of respondents achieved grades between 1.50 and 2.00, with 39 (28.3%), 36 (26.1%), and 25 (18.1%) respondents obtaining grades of 1.50, 1.75, and 2.00, respectively. Grades of 2.25, 2.50, and 2.75 were achieved by smaller proportions of respondents, with 17 (12.3%), 3 (2.2%), and 9 (6.5%) respondents, respectively. Notably, all grades fall within the passing range (3.00 or better), indicating that the majority of respondents have achieved satisfactory academic performance in the ITNET-02 course.

The distribution of respondents' academic performance in the ITNET-02 course provides valuable insights into the study's analysis for the academic performance and cybersecurity awareness among BSIT students. The predominance of passing grades, with the highest grade achieved being 1.25 and the lowest passing mark set at 3.00, indicates a generally satisfactory level of academic achievement within the sample. This suggests that the majority of respondents possess the foundational knowledge and skills necessary to succeed in the ITNET-02 course, which may positively influence their overall cybersecurity awareness. Moreover, by achieving passing grades, students demonstrate their ability to comprehend and apply course material, potentially indicating a capacity for understanding and implementing cybersecurity principles in practice. Overall, the distribution of academic performance underscores the importance of considering students' academic achievements as a factor influencing their cybersecurity awareness levels and highlights the potential interplay between academic success and cybersecurity competence within the BSIT student population.

3.3. The Level of Cybersecurity Awareness among the BSIT Students

TABLE VI. ASSESSMENT OF GENERAL CYBERSECURITY KNOWLEDGE

Item Statements	Mean	Verbal Interpretation
I am aware of the different types of cyber threats (e.g., malware, phishing).	3.53	Strongly Agree
I know the importance of having strong, unique passwords for my accounts.	3.79	Strongly Agree
I understand the concept of two-factor authentication (2FA) and how it enhances security	3.55	Strongly Agree
I am familiar with basic cybersecurity practices for safe internet browsing.	3.32	Strongly Agree
I know the risks associated with downloading and installing software from untrusted sources.	3.59	Strongly Agree
Grand Mean	**3.556**	
Verbal Interpretation	**Advanced Knowledge**	

Table 6 presents the assessment of General Cybersecurity Knowledge among respondents. The table includes five item statements related to different aspects of cybersecurity awareness, along with their corresponding means and verbal interpretations. The item statements cover areas such as awareness of cyber threats, understanding the importance of strong passwords, familiarity with two-factor authentication (2FA), knowledge of basic cybersecurity practices for safe internet browsing, and awareness of risks associated with downloading software from untrusted sources. The means range from 3.32 to 3.79, with a grand mean of 3.556, indicating an overall high level of agreement with the statements.

The results of the assessment indicate that respondents generally possess a high level of cybersecurity knowledge across the evaluated areas. The means for all item statements are above 3.0, indicating a tendency towards agreement or "Strongly Agree" with the statements. This suggests that respondents are well-informed about various cybersecurity topics, including different types of cyber threats, password security, two-factor authentication, safe internet browsing practices, and risks associated with downloading software from untrusted sources.

These results have significant implications for understanding the academic performance and cybersecurity awareness levels. A high level of cybersecurity knowledge among students suggests that they are equipped with the necessary skills and awareness to navigate the digital landscape safely and securely. Research studies emphasize the importance of cybersecurity education among students to protect them from various cybercrimes like cyberbullying, hacking, phishing, identity theft, and online scams [13, 14]. This, in turn, may positively influence their academic performance by mitigating potential cybersecurity risks that could disrupt their learning activities. Additionally, a strong foundation in cybersecurity awareness may contribute to a more proactive and responsible approach to using technology, fostering a conducive environment for academic success. Therefore, integrating cybersecurity education into academic curricula and promoting awareness among students could be beneficial for enhancing both academic performance and cybersecurity resilience within educational institutions.

TABLE VII. ASSESSMENT OF AWARENESS OF PHISHING AND SOCIAL ENGINEERING

Item Statements	Mean	Verbal Interpretation
I can recognize common signs of phishing emails (e.g., suspicious links, requests for personal information).	3.44	Strongly Agree
I am cautious about sharing personal information on social media platforms.	3.63	Strongly Agree

I know how to verify the authenticity of emails from unknown senders.	3.29	Strongly Agree
I am aware of social engineering tactics used to manipulate people into giving away confidential information.	3.14	Agree
I understand the importance of not clicking on links or downloading attachments from unknown sources.	3.66	Strongly Agree
Grand Mean	**3.432**	
Verbal Interpretation	**Very Aware**	

Table 7 presents the Assessment of Awareness on Phishing and Social Engineering among respondents. It includes item statements related to recognizing phishing emails, cautiousness about sharing personal information on social media, verifying the authenticity of emails, awareness of social engineering tactics, and the importance of avoiding unknown sources for links or attachments. Each item statement is accompanied by its mean score and a verbal interpretation.

The results indicate a high level of awareness among respondents regarding phishing and social engineering. The mean scores for all item statements are notably above 3.0, with the grand mean reaching 3.432, suggesting an overall high level of awareness. Specifically, respondents strongly agree with statements related to recognizing phishing emails, being cautious about sharing personal information on social media, and understanding the importance of avoiding unknown sources for links or attachments. However, there is a slightly lower level of agreement with statements regarding verifying the authenticity of emails from unknown senders and awareness of social engineering tactics. Despite this, the overall mean still indicates a high level of awareness across all aspects assessed.

These results have implications for understanding the academic performance and cybersecurity awareness. A high level of awareness among respondents suggests that they may possess the knowledge and skills necessary to protect themselves against phishing attacks and social engineering tactics. The study of authors [15] have shown a significant correlation between low cybersecurity awareness levels and increased cybercrime rates, emphasizing the importance of awareness in preventing cyber threats. This heightened awareness could potentially contribute to better cybersecurity practices among students, which may positively impact their overall academic performance. Additionally, these findings underscore the importance of integrating cybersecurity education and awareness programs into academic curricula to further enhance students' understanding and preparedness in this critical area.

TABLE VIII. ASSESSMENT OF SAFE ONLINE PRACTICES

Item Statements	**Mean**	**Verbal Interpretation**
I regularly update my software and applications to protect against vulnerabilities.	3.38	Strongly Agree
I use antivirus software to scan my computer for malware and other threats.	3.25	Strongly Agree
I avoid using public Wi-Fi for sensitive transactions, such as online banking.	3.36	Strongly Agree
I regularly back up important data to prevent loss in case of a cyber-attack.	3.33	Strongly Agree
I am aware of the importance of logging out of accounts after use, especially on shared devices.	3.65	Strongly Agree
Grand Mean	**3.394**	
Verbal Interpretation	**Advanced Safe Online Practices**	

Table 8 presents the respondents' self-assessment of their adherence to safe online practices. The table lists various statements related to cybersecurity behaviors and the corresponding mean scores, alongside their verbal interpretations. The mean scores range from 3.25 to 3.65, with all items interpreted as "Strongly Agree." The grand mean of 3.394 is verbally interpreted as "Advanced Safe Online Practices."

The results indicate that respondents generally exhibit strong agreement with the statements regarding safe online practices. The highest mean score (3.65) is associated with awareness of the importance of logging out of accounts after use, especially on shared devices. Other practices such as regularly updating software (mean = 3.38), avoiding public Wi-Fi for sensitive transactions (mean = 3.36), regularly backing up important data (mean = 3.33), and using antivirus software (mean = 3.25) also received high ratings, suggesting that respondents are knowledgeable about and committed to maintaining safe online behaviors.

These results have important implications for the study of the academic performance and cybersecurity awareness levels. The high self-reported adherence to safe online practices suggests that respondents possess a substantial understanding of essential cybersecurity measures. This high level of cybersecurity awareness could potentially correlate with better academic performance, as students who practice safe online behaviors are less likely to experience disruptions caused by cyber threats. Consequently, the findings emphasize the need for continued education and reinforcement of cybersecurity practices to support both academic success and digital safety among IT students.

TABLE IX. ASSESSMENT OF CYBERSECURITY BEHAVIORS AND ATTITUDES

Item Statements	**Mean**	**Verbal Interpretation**
I feel confident in my ability to protect my personal information online.	3.43	Strongly Agree
I take cybersecurity seriously and make an effort to stay informed about new threats.	3.33	Strongly Agree
I believe that my actions can significantly impact my cybersecurity.	3.43	Strongly Agree
I regularly review and update my privacy settings on social media accounts.	3.33	Strongly Agree
I am proactive in educating myself about cybersecurity best practices.	3.35	Strongly Agree
Grand Mean	**3.374**	
Verbal Interpretation	**Very Good Cybersecurity Behaviors and Attitudes**	

Table 9 presents an assessment of respondents' cybersecurity behaviors and attitudes. It includes various item statements related to their confidence in protecting personal information, their seriousness about cybersecurity, and their proactive measures in staying informed and updating privacy settings. Each statement's mean score is provided along with a verbal interpretation. The table also presents a grand mean score and an overall verbal interpretation of the respondents' cybersecurity behaviors and attitudes.

The mean scores for each statement indicate that respondents generally "Strongly Agree" with the positive cybersecurity behaviors and attitudes described. For instance, respondents show strong confidence in their ability to protect personal information online (Mean = 3.43) and believe their actions can significantly impact their cybersecurity (Mean = 3.43). They also demonstrate a proactive approach by regularly reviewing privacy settings on social media (Mean = 3.33) and staying informed about new threats (Mean = 3.33). The grand mean score of 3.374, with a verbal interpretation of "Very Good Cybersecurity Behaviors and Attitudes," suggests that, overall, respondents exhibit commendable cybersecurity practices and a positive attitude toward maintaining cybersecurity.

The findings from Table 9 have significant implications for understanding the academic performance and cybersecurity awareness levels among IT students. The high mean scores and positive verbal interpretations suggest that respondents possess a strong awareness of cybersecurity practices and attitudes. This heightened awareness likely contributes positively to their academic performance, as being well-informed about cybersecurity can enhance their ability to engage with course material effectively, particularly in IT-related subjects. Additionally, the proactive and serious attitude towards cybersecurity indicated by these results underscores the importance of integrating cybersecurity education into the academic curriculum. This integration could further improve students' performance and preparedness for real-world challenges, emphasizing the critical role of cybersecurity awareness in their overall educational experience.

TABLE X. ASSESSMENT OF INCIDENT RESPONSE AWARENESS

Item Statements	**Mean**	**Verbal Interpretation**
I know what steps to take if I suspect that my computer has been infected with malware.	3.19	Agree
I am familiar with the procedures for reporting a cybersecurity incident at my institution.	2.96	Agree
I understand the importance of notifying relevant authorities immediately after discovering a potential breach.	3.25	Strongly Agree
I know how to identify and respond to a potential data breach involving my personal information.	3.12	Agree
I am aware of the resources available to help me recover from a cyber-attack.	3.17	Agree
Grand Mean	**3.138**	
Verbal Interpretation	**Good Incident Response Awareness**	

The table above presents the assessment of respondents' awareness and preparedness regarding incident response in cybersecurity. Each item statement is rated on a scale, with means calculated for each statement and an overall grand mean provided. The verbal interpretations range from "Agree" to "Strongly Agree," with individual item means varying from 2.96 to 3.25.

The results show that respondents generally agree with the statements related to incident response awareness, with mean scores indicating a solid understanding of various aspects of incident response. The highest mean score of 3.25 (Strongly Agree) is associated with the importance of notifying relevant authorities immediately after discovering a potential breach, reflecting a strong awareness of the critical nature of timely reporting in incident response. The other items, with means ranging from 2.96 to 3.19, indicate that respondents are reasonably knowledgeable about steps to take if infected with malware, procedures for reporting incidents, identifying and responding to data breaches, and resources for recovery post-attack. The grand mean of 3.138 suggests that overall, respondents possess good incident response awareness.

The findings imply that respondents have a decent level of incident response awareness, which is crucial for mitigating the effects of cybersecurity threats. In the context of understanding the academic performance and cybersecurity awareness, this result indicates that students with better incident response knowledge might perform better academically in cybersecurity-related courses. This is because their preparedness and proactive approach to managing cyber incidents could contribute to a deeper understanding and practical application of cybersecurity principles. Consequently, the study's exploration of this relationship can benefit from acknowledging that strong incident response awareness potentially enhances both theoretical and practical cybersecurity competencies among IT students. This insight can help tailor educational strategies to further strengthen incident response training, thereby improving both cybersecurity awareness and academic outcomes.

IV. CONCLUSIONS

In conclusion, this study highlights the critical importance of cybersecurity awareness among IT students, particularly in relation to their academic performance. The analysis of demographic profiles, academic achievements, and various aspects of cybersecurity knowledge and practices among first-year BSIT students at the Nueva Ecija University of Science and Technology reveals significant insights. The findings suggest that a considerable portion of the students possess a solid foundation in general cybersecurity knowledge, phishing awareness, safe online practices, cybersecurity behaviors and attitudes, and incident response awareness. The predominance of passing grades indicates a satisfactory level of academic performance, which may be influenced by their understanding and implementation of cybersecurity measures. These results underscore the necessity of integrating comprehensive cybersecurity education into academic curricula to equip students with the essential skills to navigate the digital landscape securely.

Furthermore, the study's results indicate that while there is a high level of cybersecurity awareness among the respondents, there remains a need for continuous enhancement and targeted interventions to address specific gaps. For instance, a more balanced gender representation in future studies could provide a broader understanding of the cybersecurity awareness and academic performance relationship across different demographics. Additionally, the varying levels of prior experience in networking or cybersecurity among students highlight the need for tailored educational strategies to support those with less background knowledge. By focusing on these areas, educational institutions can better prepare students for the cybersecurity challenges of the digital age, ultimately contributing to improved academic performance and a more secure digital environment.

V. RECOMMENDATIONS

Based on the findings of this study, several recommendations are proposed to further enhance the instructional quality of cybersecurity education for IT students:

Firstly, integrating comprehensive cybersecurity modules into the ITNET-02 course is crucial. These modules should cover fundamental cybersecurity principles, safe online practices, and effective incident response strategies. By embedding these topics as supplemental unit throughout the academic program, students can develop a solid understanding of cybersecurity from the outset of their studies.

Secondly, offering ongoing cybersecurity education through workshops, seminars, and participation in cybersecurity competitions is essential. These activities not only keep students updated on emerging threats but also provide practical experience in applying cybersecurity principles. Such initiatives can foster a proactive approach to cybersecurity among students.

Thirdly, there is a need to focus specifically on promoting safe online practices and enhancing incident response capabilities. Training sessions should emphasize the importance of secure behaviors online, such as using strong passwords and avoiding suspicious links. Additionally, educating students on how to effectively respond to cyber incidents can mitigate potential risks and disruptions.

Moreover, incorporating engaging learning methods, such as interactive simulations and gamified activities, can make cybersecurity education more engaging and effective. These methods can help reinforce learning and improve retention of cybersecurity concepts among students.

Additionally, leveraging student performance data to identify areas of improvement and adjust teaching strategies accordingly is crucial. Analyzing academic performance data can provide insights into where students may need additional support or focus, ensuring that educational efforts are targeted and effective.

Lastly, supporting continuous professional development for educators in cybersecurity is essential. Providing training on current cybersecurity trends, teaching methodologies, and effective use of educational technology can empower educators to deliver high-quality cybersecurity education.

REFERENCES

[1.] M. Gracy, B. R. Jeyavadhanam, P. K. Babu, S. H. Karthick, and R. Chandru, "Growing Threats Of Cyber Security: Protecting Yourself In A Digital World," in 2023 International Conference on Networking and Communications (ICNWC), 2023, IEEE, doi: 10.1109/icnwc57852.2023.10127398.

[2.] M. Paliwal, "A review on cyber security," in INSTRUMENTATION ENGINEERING, ELECTRONICS AND TELECOMMUNICATIONS – 2021 (IEET-2021): Proceedings of the VII International Forum, AIP Publishing, 2023, doi: 10.1063/5.0101190.

[3.] T. Untawale, "Importance of Cyber Security in Digital Era," in International Journal for Research in Applied Science and Engineering Technology, vol. 9, no. 8, pp. 963-966, International Journal for Research in Applied Science and Engineering Technology (IJRASET), 2021. doi: 10.22214/ijraset.2021.37519.

[4.] G. Kumar, S. K. Pandey, N. Varshney, A. Kumar, M. Kumar, and K. U. Singh, "Cybersecurity Education: Understanding the knowledge gaps based on cyber security policy, challenge, and knowledge," in 2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT), 2023, IEEE, doi: 10.1109/csnt57126.2023.10134610.

[5.] F. Quayyum, "Collaboration between parents and children to raise cybersecurity awareness," in European Interdisciplinary Cybersecurity Conference, EICC 2023, ACM, 2023. doi: 10.1145/3590777.3590802.

[6.] S. Alrobaian, S. Alshahrani, and A. Almaleh, "Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation," in Big Data and Cognitive Computing, vol. 7, no. 2, p. 73, MDPI AG, 2023. doi: 10.3390/bdcc7020073.

[7.] H. S. Berry, "Survey of the Challenges and Solutions in Cybersecurity Awareness Among College Students," in 2023 11th International Symposium on Digital Forensics and Security (ISDFS), 2023, IEEE, doi: 10.1109/isdfs58141.2023.10131851.

[8.] W. C. H. Hong, C. Chi, J. Liu, Y. Zhang, V. N.-L. Lei, and X. Xu, "The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates," in Education and Information Technologies, vol. 28, no. 1, pp. 439-470, Springer Science and Business Media LLC, 2022. doi: 10.1007/s10639-022-11121-5.

[9.] M. Khader, M. Karam, and H. Fares, "Cybersecurity Awareness Framework for Academia," in Information, vol. 12, no. 10, p. 417, MDPI AG, 2021. doi: 10.3390/info12100417.

[10.] M. B. Hoang T., D. Dang-Pham, A.-P. Hoang, B. Le Gia, and M. Nkhoma, "Network Analytics for Improving Students' Cybersecurity Awareness in Online Learning Systems," in 2020 RIVF International Conference on Computing and Communication Technologies (RIVF), 2020, IEEE, doi: 10.1109/rivf48685.2020.9140781.

[11.] G. Q. Wijaya, "Gender Roles and Culture: Female Students' Interest in Information Technology Major and Career," in K@ta Kita, vol. 10, no. 1, pp. 132-140, Petra Christian University, 2022. doi: 10.9744/katakita.10.1.132-140.

[12.] Y. Zhang, T. Gros, and E. Mao, "Gender Disparity in Students' Choices of Information Technology Majors," in Business Systems Research Journal, vol. 12, no. 1, pp. 80-95, Walter de Gruyter GmbH, 2021. doi: 10.2478/bsrj-2021-0006.

[13.] C. S. Lee and Y. T. Chua, "The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States," in Crime & Delinquency, SAGE Publications, 2023. doi: 10.1177/00111287231180093.

[14.] C. Hygeia S. Toso, A. J. Jumalon, J. A. R. Magadan, A. B. Alvarico, and J. F. Cuevas Jr, "Cybercrime Awareness Among Senior High School Students," in Mediterranean Journal of Basic and Applied Sciences, vol. 07, no. 02, pp. 160-176, Nemeth Publishers, 2023. doi: 10.46382/mjbas.2023.7218.

[15.] F. K. Mupila, H. Gupta, and A. Bhardwaj, "An Empirical Study on Cyber Crimes and Cybersecurity Awareness," Research Square Platform LLC, 2023. doi: 10.21203/rs.3.rs-3037289/v1.