International Research Journal of MMC (IRJMMC)
ISSN 2717-4999 (Online) | 2717-4980 (Print)
Volume 6, Issue 5 | December 2025

Cybersecurity Awareness and Practices of Students at Makawanpur Multiple Campus, Nepal

Shreeraj Khatiwada[1]

[1]Assistant Lecturer of Information & Technology
Makawanpur Multiple Campus, Hetauda

Corresponding Author
Shreeraj Khatiwada
Email: shreerajhtd@gmail.com

To Cite this article: Khatiwada, S. (2025). Cybersecurity Awareness and practices of students at Makawanpur Multiple Campus, Nepal. *International Research Journal of MMC, 6*(5), 26–37. https://doi.org/10.3126/irjmmc.v6i5.89028

Submitted: 28 August 2025 **Accepted:** 15 December 2025 **Published:** 31 December 2025

Abstract

This study explores the awareness and practices of cybersecurity among students at Makawanpur Multiple Campus, Hetauda, Nepal. With increasing dependence on digital platforms for learning and communication, students face growing risks such as phishing, hacking, and data breaches. A quantitative, descriptive cross-sectional survey was conducted in year 2025 A.D. among 148 students from +2 Computer Science and Bachelor IT programs using a structured questionnaire through convenience sampling. Data were collected using a structured questionnaire with close-ended and open-ended questions and analyzed using descriptive statistics, including frequency distributions, percentages, and mean scores. Findings reveal that while some students possess basic knowledge of cybersecurity, the majority lack sufficient awareness of safe practices including password management, device protection, and secure online behavior. More than one-third of students reported experiencing cyber incidents, yet most expressed low confidence in handling such threats. Despite these challenges, a large majority showed strong interest in workshops, training, and awareness programs. The study highlights the urgent need for capacity-building initiatives, curriculum integration, awareness campaigns, and institutional support. These measures can bridge the gap between knowledge and practice, fostering a safer digital learning environment for students in higher education. The findings of this study will benefit students, educators, campus administration, and policymakers by providing insights to enhance cybersecurity awareness and practices.

Keywords: cybersecurity awareness, cybersecurity practices, students, higher education, cyber incidents, digital literacy

1. Introduction

The twenty-first century has brought rapid integration of digital technologies into education, communication, and everyday life. In academic settings, students depend heavily on laptops, smartphones, and online platforms for learning, collaboration, and personal use. Social media, cloud-based applications, and e-payment systems are part of their daily routines. While these technologies provide convenience and new opportunities, they also expose

students to cybersecurity risks such as phishing, identity theft, scams, account hacking, and data breaches (Alshaikh, 2020). As students are among the most active internet users, their awareness and adoption of safe practices are critical for protecting both academic and personal information.

Cybersecurity has therefore emerged as an essential component of modern education. It is no longer limited to IT professionals but is relevant to every student who engages with digital platforms. However, research suggests that young people often underestimate cybersecurity threats. Many of them use weak or repetitive passwords, ignore updates, and share information on unsafe channels (Hadlington, 2017). Their constant online presence makes them attractive targets for cybercriminals. For this reason, developing cybersecurity literacy is vital not only for protecting individual students but also for strengthening institutional security in higher education (Walton et al., 2021).

Globally, awareness programs and policies have been introduced to address this challenge. Universities in developed countries often conduct workshops, training, and awareness campaigns to prepare students for cyber risks (Towhidi & Pridmore, 2023). In contrast, many developing countries face constraints in integrating cybersecurity into education. Nepal illustrates this challenge clearly. Internet penetration and digital service use have expanded rapidly in recent years, supported by growing access to smartphones, e-payments, and e-learning platforms. However, cybersecurity education remains underdeveloped. While national policies highlight digital transformation, structured programs on cybersecurity awareness are still limited, especially at the institutional level (Dhungana et al., 2023).

At the campus level, this issue becomes even more pressing. Many higher education institutions in Nepal lack dedicated infrastructure, expertise, and formal strategies for building cybersecurity awareness. Students, particularly those in early academic years, receive little formal guidance on safe practices such as strong password management, multi-factor authentication, or recognizing suspicious emails (Bhandari, 2025). As a result, there is a gap between technological usage and students' ability to engage securely. Bridging this gap is essential to safeguard young learners who increasingly rely on digital platforms for academic and personal activities.

Makawanpur Multiple Campus, located in Hetauda, provides a relevant case for such investigation. The campus accommodates a diverse student population and offers +2 Computer Science and Bachelor-level IT programs. These students interact with computers, networks, and digital platforms on a daily basis, making cybersecurity particularly important. Despite this, it is unclear to what extent they are aware of cyber risks or apply protective practices. Examining their knowledge, attitudes, and behaviors provides an opportunity to better understand local realities and guide improvements in cybersecurity literacy.

The value of this research lies in its multiple beneficiaries. Students can gain awareness of their own vulnerabilities and adopt safer habits. The campus administration can design targeted interventions such as workshops, awareness campaigns, and technical support mechanisms. Educators can integrate cybersecurity more systematically into curricula, while policymakers may use the findings to strengthen national strategies tailored to young, tech-active populations outside major cities. Ultimately, the study provides localized insights into an increasingly global concern and contributes to the broader aim of ensuring digital safety in education.

This study is limited to +2 Computer Science and Bachelor IT students at Makawanpur Multiple Campus, Hetauda, Nepal. It focuses on their cybersecurity awareness and practices, such as password management, device protection, and online behavior. Only students who voluntarily participated in the survey were included, and data were collected at a single point in time.

In summary, the digitalization of education has expanded both opportunities and risks for students. While global attention to cybersecurity is growing, evidence from Nepal remains limited, particularly at the campus level. With Makawanpur Multiple Campus serving as a case study, this research examines students' awareness, practices, and experiences related to cybersecurity, aiming to contribute practical recommendations for improving digital safety in academic environments.

1.1 Research Objective

To assess cybersecurity awareness and practices among students of Makawanpur Multiple Campus and recommend measures for improvement.

1.2 Research Question

What is the current level of cybersecurity awareness and practices among students of Makawanpur Multiple Campus, and what measures can be implemented to enhance their cybersecurity literacy?

1.3 Literature Review

Gabra et al. (2020) investigated cybersecurity awareness among university students in Nigeria. The study found that although students possessed basic knowledge of cybersecurity, they lacked practical skills to protect their data effectively. Moreover, most universities did not provide active awareness programs. Despite these deficiencies, students expressed strong interest in learning more about cybersecurity. These findings highlight the potential effectiveness of targeted awareness programs, which is highly relevant for designing interventions in the context of Makawanpur Multiple Campus.

Švábenský et al. (2021) analyzed cybersecurity knowledge and skills developed through Capture the Flag (CTF) challenges. Their study of 15,963 solutions showed that CTFs effectively teach technical skills such as cryptography and network security but largely neglect human aspects like social engineering and cybersecurity awareness. The authors recommended integrating non-technical topics into such challenges to prepare students for contemporary cyber threats. These insights are relevant for improving practical cybersecurity exercises in academic settings.

The study by Dhungana et al. (2023) investigated cybersecurity challenges and awareness among multi-generational learners in Nepal, including 891 students and 157 teachers. The researchers found that schools' cybersecurity support systems were weak, and teachers had limited competencies to safeguard students from cyber risks. The study highlighted a significant gap between students' and teachers' cybersecurity awareness, emphasizing that poor cybersecurity acts as a barrier to educational quality. These findings suggest that enhancing cybersecurity awareness at both student and teacher levels is crucial, providing a strong rationale for examining awareness and practices in a local campus setting.

Al-Sherideh et al. (2023) investigated the impact of cybersecurity measures in e-learning platforms on students and educators in Jordan. The study revealed that implementing access controls, encryption, software updates, and student training significantly improved engagement and participation in e-learning. The authors emphasized that comprehensive cybersecurity strategies enhance both protection and student confidence in digital learning, highlighting the importance of combining technical measures with awareness programs.

Du (2023) conducted a survey on cybersecurity awareness among 384 undergraduate students at Yunnan University of Finance and Economics in China, focusing on knowledge, privacy, password management, and trust. The study found that students who received formal or informal training exhibited higher awareness levels, while major had no significant effect.

Learning approaches and gender were significantly associated with awareness, emphasizing the importance of targeted training programs for improving cybersecurity practices.

According to Bottyan (2023), the integration of ICT in education has increased vulnerability to cyber threats among students and educational institutions. The study highlighted the need for protective measures to safeguard personal data, intellectual property, and ensure continuity in digital learning. The author emphasized that fostering information security awareness is crucial for developing responsible and security-conscious digital competence among students.

A study by Fattah et al. (2023) examined the relationship between knowledge, attitude, behavior, and training in shaping cybersecurity awareness among university students. Using a quantitative survey of 64 students and analysis through PLS-SEM, the study found that knowledge, attitude, behavior, and training all positively influenced students' cybersecurity awareness. The authors concluded that targeted interventions, including structured training programs, could effectively enhance cybersecurity knowledge and safe online practices among students.

Lohani and Kumar (2024) examined cybersecurity awareness, knowledge, and practices among students, faculty, and administrators in Nepalese higher education institutions. The study found variability in awareness across stakeholder groups and identified challenges in promoting secure behavior. The authors stressed the importance of structured training programs, institutional strategies, and policy interventions to protect the academic community from evolving cyber threats. This research is relevant for the present study as it highlights the influence of institutional support on students' cybersecurity behavior.

A study conducted by Bhandari (2025) examined cybersecurity awareness and knowledge of legal frameworks among university students in Nepal. The study found that while 67.2% of students were familiar with the concept of hacking, only 46.9% were aware of Nepal's cybersecurity legal framework, indicating significant gaps in awareness of protective measures. The author emphasized the need for legal education, practical cybersecurity training, curriculum integration, and institutional policies to enhance students' ability to safeguard their digital interactions. These findings underscore the need to evaluate similar gaps among students in Makawanpur Multiple Campus, particularly regarding legal and practical cybersecurity understanding.

Research conducted by Adhikari et al. (2025) explored factors influencing cybersecurity practices across Nepalese organizations, including education, healthcare, and SMEs. The study revealed that limited resources, lack of skilled personnel, and insufficient technological infrastructure hinder effective cybersecurity implementation. While private organizations demonstrated higher awareness, small and medium enterprises were particularly vulnerable. The authors emphasized the need for context-specific solutions and institutional support, which may also inform strategies for improving cybersecurity practices among students and staff at higher education institutions.

1.4 Research Gap

The existing literature on cybersecurity awareness and practices among students primarily highlights the general lack of awareness and insufficient protective behaviors but leaves gaps in understanding the specific factors that influence these gaps in local educational contexts. Most studies focus on either general knowledge of cybersecurity, legal frameworks, or institutional policies, but few explore how students actually practice safe online behaviors, such as password management, device protection, and safe e-payment use. Moreover, while some research has examined cybersecurity awareness among university students, few studies have looked into the combined perspectives of +2 Computer Science and Bachelor IT students in Nepal, particularly in campus-specific settings like Makawanpur Multiple Campus. This

study aims to address these gaps by assessing both the awareness and practical cybersecurity behaviors of students, identifying challenges they face, and suggesting context-specific interventions to improve cybersecurity literacy and safe digital practices in higher education environments.

2. Methods

2.1 Research Design

This study employed a quantitative, descriptive, cross-sectional survey design to assess the awareness and practices of cybersecurity among students. The design was appropriate to capture students' perceptions, knowledge, and behaviors regarding cybersecurity within a defined time frame.

2.2 Study Area and Population

The research was conducted in 2025 AD among students of Makawanpur Multiple Campus, Hetauda, Nepal, focusing specifically on those enrolled in the +2 Computer Science and Bachelor-level Information Technology (IT) programs, as these groups are more directly engaged with computing and digital technologies.

2.3 Sample and Sampling Technique

The target population consisted of 276 students enrolled in the +2 Computer Science and Bachelor IT programs. A total of 154 responses were collected through the questionnaire, and after data preprocessing and cleaning to remove incomplete or invalid responses, 148 responses were finalized for analysis. A purposive sampling technique was applied to ensure the study focused specifically on students from the computer science and IT streams, as they are directly related to the topic of cybersecurity awareness and practices.

2.4 Data Collection Procedure

Data was collected using a structured questionnaire consisting of 14 close-ended questions and 1 open-ended question, designed to capture demographic details, levels of cybersecurity awareness, common practices, experiences with cyber incidents, and recommendations for improvement. The questionnaire was prepared in Google Forms and distributed digitally to students through online platforms. Data collection was conducted over several days, ensuring voluntary participation. Only students who gave informed consent at the beginning of the form were included in the study.

2.5 Data Analysis

The finalized dataset of 148 responses was analyzed using Python programming language. The analysis was limited to descriptive statistics, including frequency distributions, percentages, and mean scores. These measures were used to summarize demographic characteristics, awareness levels, practices, and students' experiences with cybersecurity.

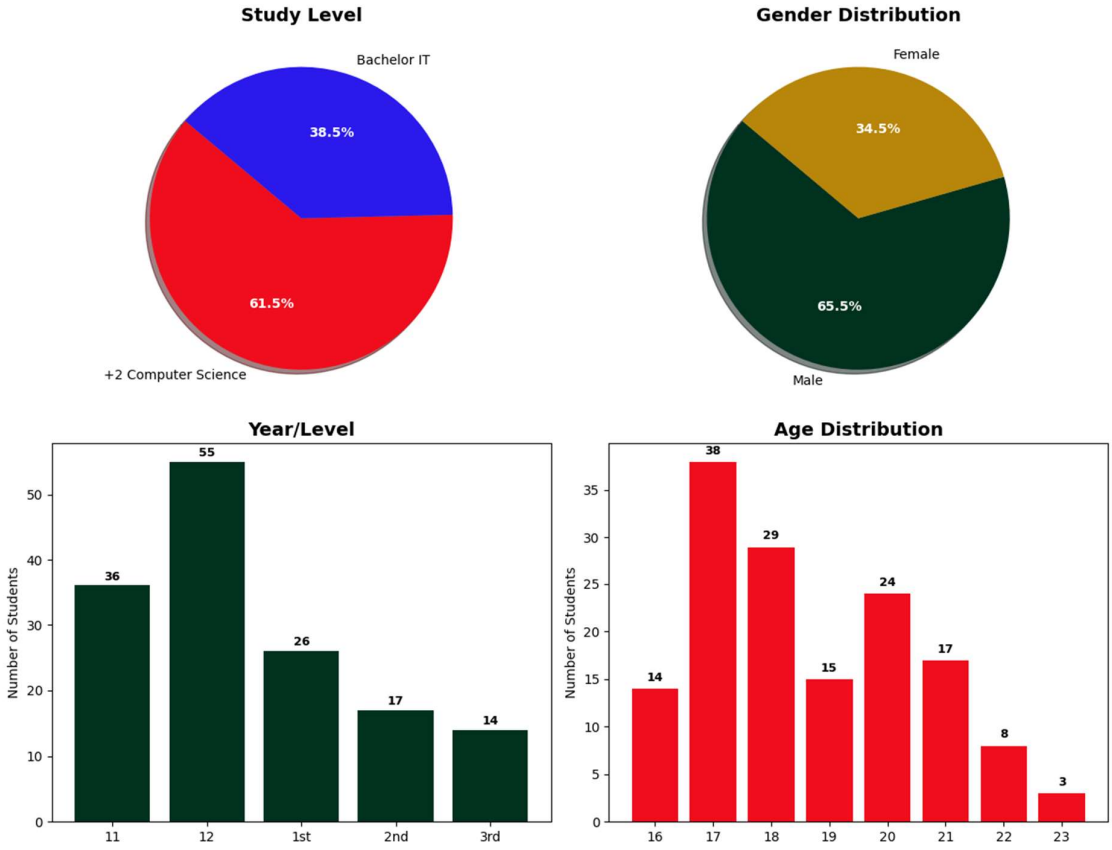
2.6 Ethical Considerations

Ethical standards were maintained throughout the study. Participation was voluntary, and respondents were required to provide informed consent before accessing the questionnaire. Anonymity and confidentiality of participants were strictly ensured, and the collected data was used exclusively for academic purposes.

3. Results and Discussion

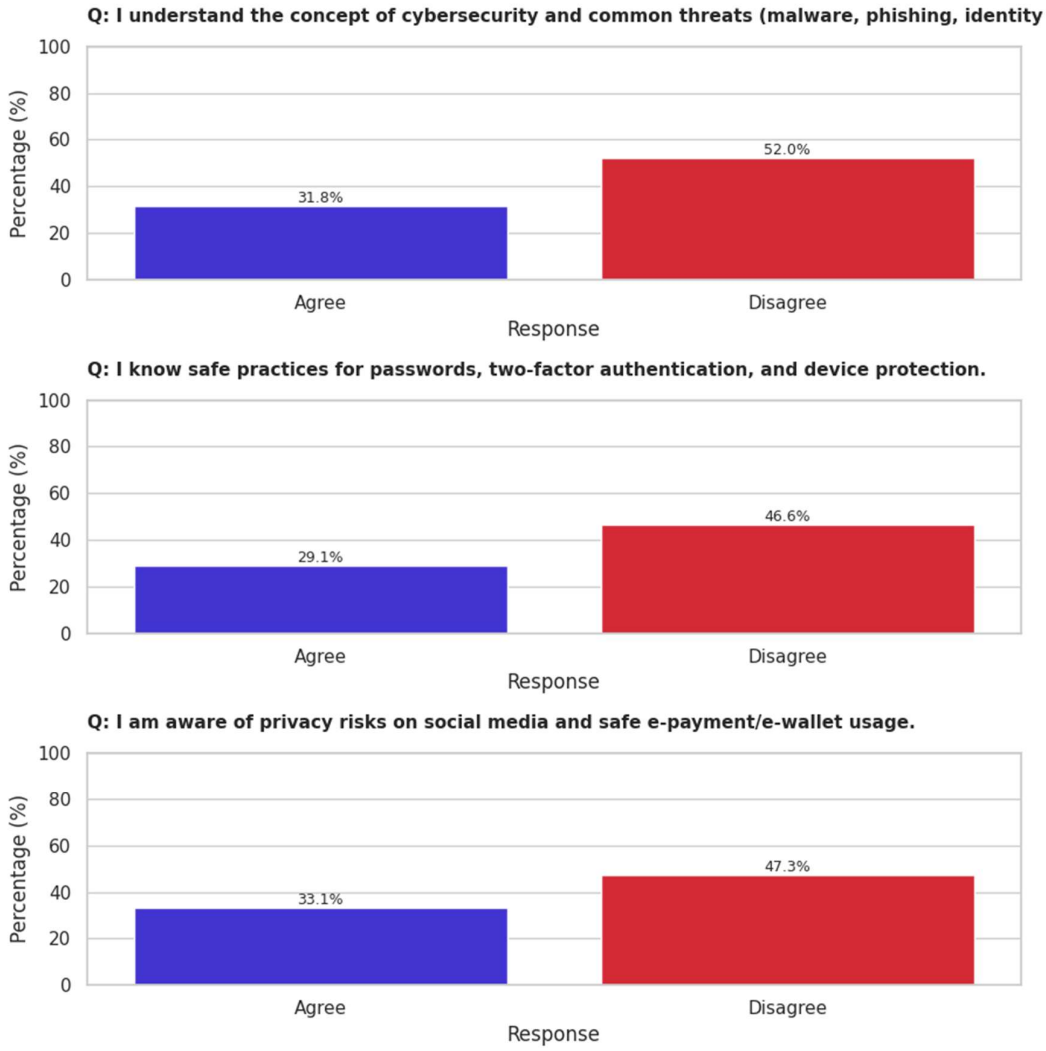
This section presents the findings of the study, focusing on the awareness and practices of cybersecurity among students of Makawanpur Multiple Campus. The results are analyzed in relation to the research questions, which explore the levels of cybersecurity knowledge, common digital practices, experiences with cyber incidents, and students' perceptions of effective measures to enhance cybersecurity literacy. Data visualization techniques, including charts, graphs, and descriptive statistical analyses, are employed to clearly and effectively present the findings.

Figure 1: *Demographics Overview*



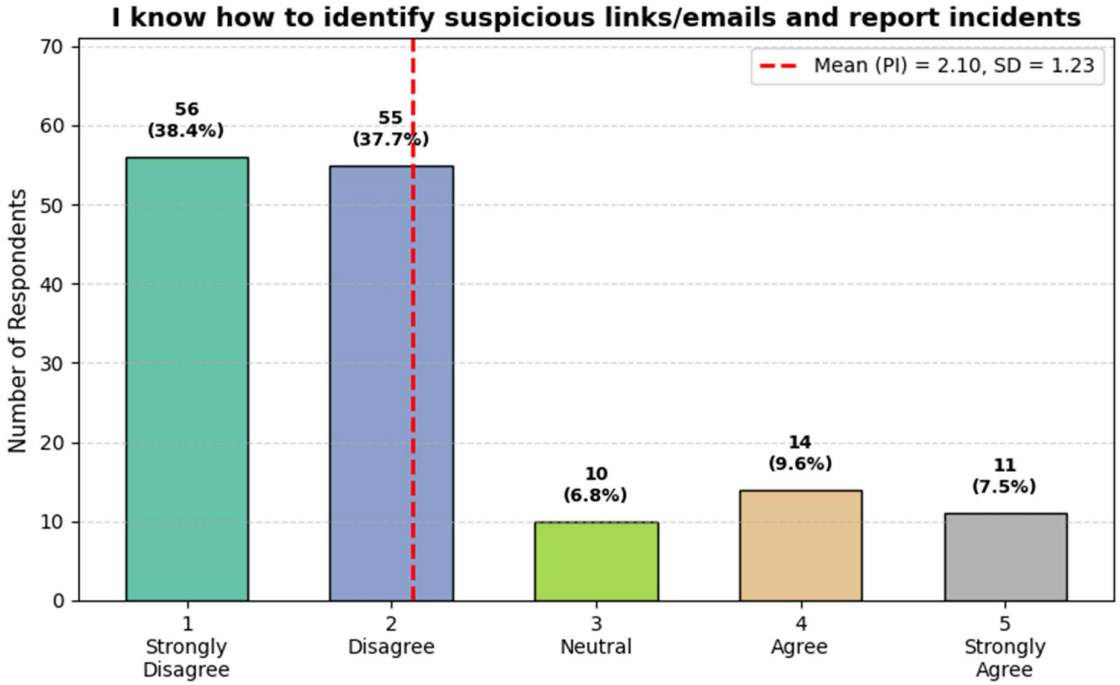
A total of 148 students participated in the study, representing different age groups (16–23 years)**,** levels of study (+2 Computer Science 61.5% and Bachelor IT 38.5%)**,** and academic years**.** The majority were male (65.5%)**,** and most came from the younger cohorts of +2 level, particularly Grade 12. This diverse participation ensured representation across gender, study levels, and age groups, providing a broad basis for assessing cybersecurity awareness and practices.

Figure 2: *Cybersecurity Awareness*



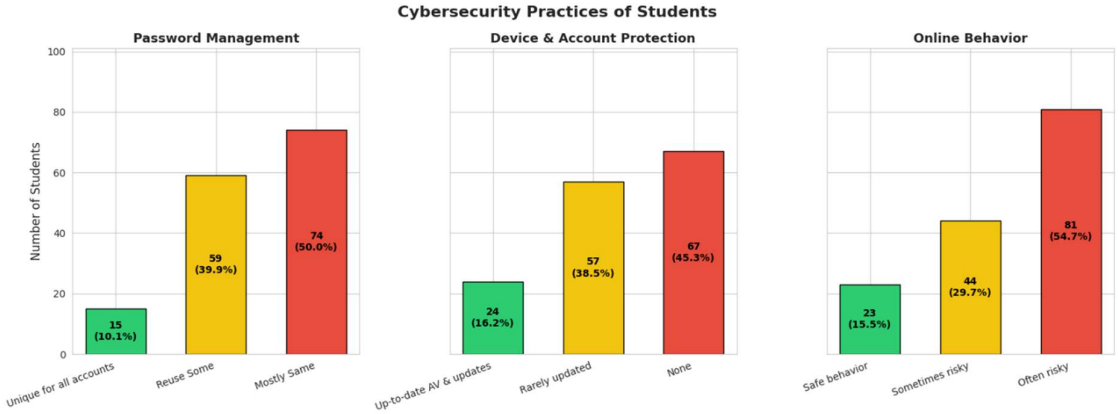
Findings indicate limited awareness of cybersecurity among students. Only 31.8% agreed that they understood the concept of cybersecurity and common threats, while 52.0% disagreed. Similarly, just 29.1% reported knowledge of safe practices such as strong passwords, two-factor authentication, and device protection, compared to 46.6% who disagreed. Awareness was slightly higher for privacy risks on social media and safe e-payment usage, with 33.1% agreeing, but still fewer than the 47.3% who disagreed. Overall, the results suggest that while a portion of students have basic awareness, a majority lack sufficient understanding of key cybersecurity concepts and practices.

Figure 3: *Cybersecurity Practices*



The findings show limited ability among students to identify suspicious links or emails and report incidents. A large majority (76.1%) disagreed or strongly disagreed**,** while only 17.1% agreed or strongly agreed and 6.8% remained neutral**.** The mean Practice Index (PI) was 2.10 (SD = 1.23)**,** indicating that overall confidence in this practice is low, with responses leaning toward disagreement.

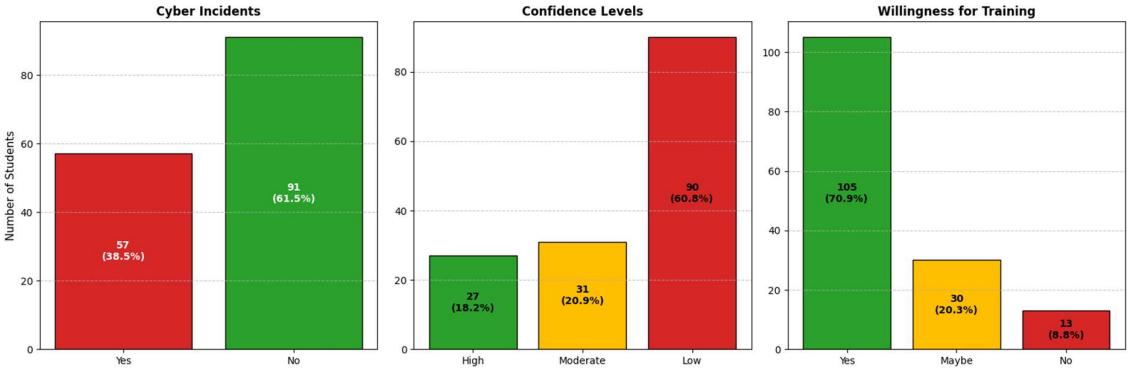
Figure 4: *Cybersecurity Practices of Students*



As shown in Figure 4, students' cybersecurity practices reveal significant weaknesses. In Password Management**,** only 10.1% used unique passwords for all accounts, while the majority reused some (39.9%) or mostly the same password (50%). In terms of Device & Account Protection**,** just 16.2% kept their systems and antivirus updated, whereas 83.8% either rarely updated or did not use protection at all. For Online Behavior**,** only 15.5% consistently practiced safe habits, while more than half (54.7%) frequently engaged in risky behaviors.

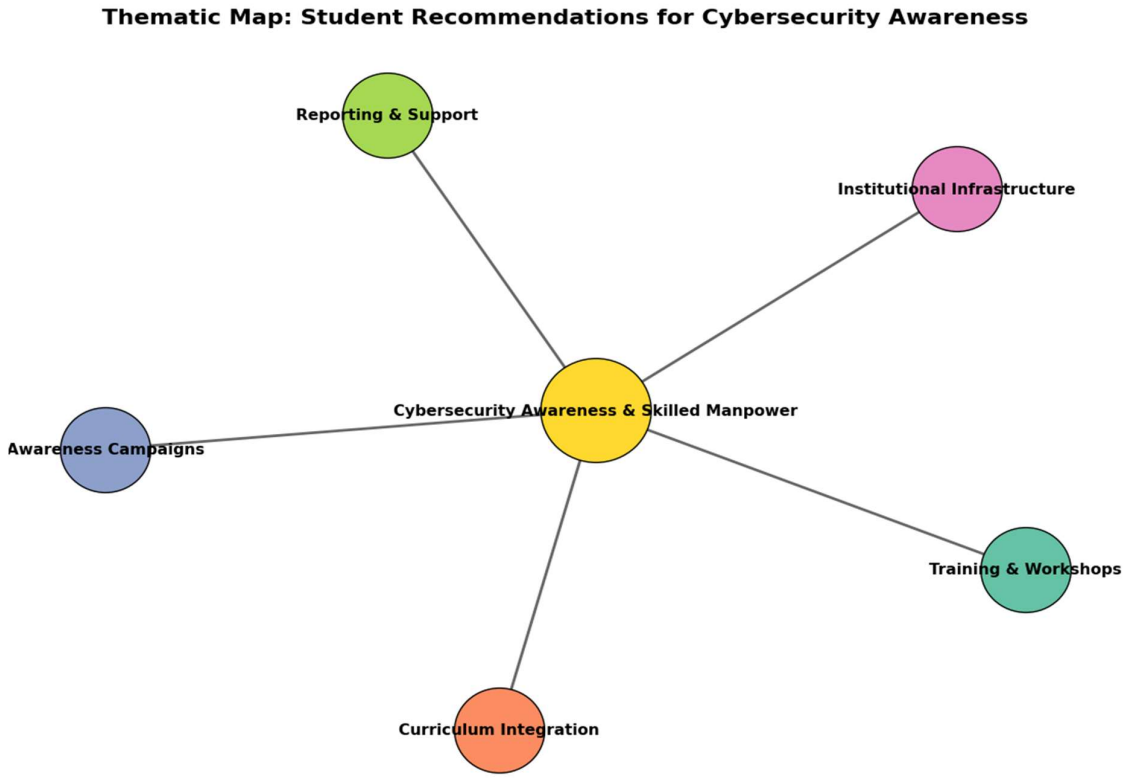
These findings highlight a considerable gap between secure practices and actual student behavior, pointing to the need for stronger awareness and training interventions.

Figure 5: *Cyber Incidents and Confidence of Students*



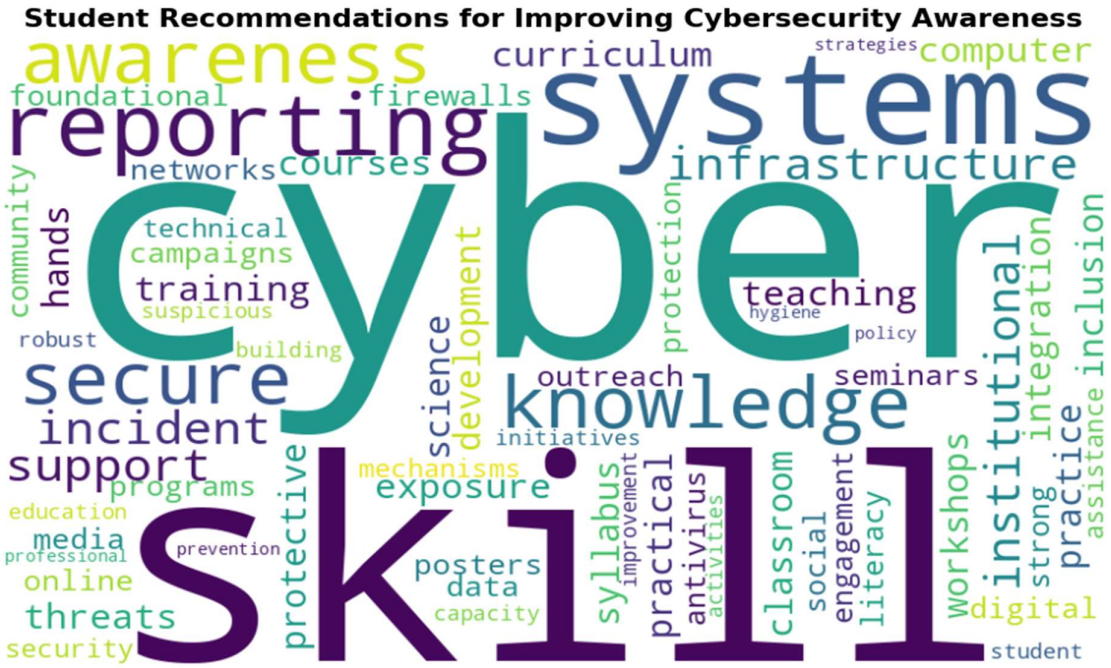
The survey findings (Figure 5) indicate that 57 students (38.5%) had experienced cyber incidents such as account hacking, scams, or data loss, while the majority, 91 students (61.5%), had not faced such issues. In terms of confidence levels, only 27 students (18.2%) felt highly confident in handling cybersecurity threats, 31 (20.9%) reported moderate confidence, and a large proportion, 90 students (60.8%), expressed low confidence. Despite these challenges, students showed strong interest in capacity building, with 105 respondents (71.0%) willing to participate in cybersecurity training or workshops, 30 (20.3%) uncertain, and only 13 (8.7%) not interested.

Figure 6: *Thematic Map*



Analysis of the open-ended responses revealed that students recommended a multi-pronged strategy for improving cybersecurity awareness and developing skilled manpower. The most frequently emphasized measure was the organization of workshops and hands-on training sessions, which were seen as crucial for providing practical exposure to real-world threats and enhancing protective skills. A second major theme was the integration of detail cybersecurity concepts into the curriculum, particularly within computer science and IT courses, to strengthen foundational knowledge. Students also highlighted the importance of awareness campaigns; through seminars, posters, digital outreach, and classroom discussions; to extend cybersecurity literacy beyond IT majors and engage the broader student community. In addition, many responses underscored the need for robust institutional IT infrastructure, suggesting that secure systems would both safeguard data and model best practices for learners. Finally, respondents recommended establishing clear incident-reporting mechanisms and technical support structures to encourage timely responses to suspicious activities or breaches.

Figure 7: *Word Cloud*



4. Conclusion

The study assessed cybersecurity awareness and practices among students of Makawanpur Multiple Campus, focusing on +2 Computer Science and Bachelor IT programs. The findings indicate that while a small portion of students have basic knowledge of cybersecurity concepts, the majority lack sufficient understanding of key areas such as password management, device protection, safe online behavior, and general cyber threats. More than one-third of students reported experiencing cyber incidents, yet most expressed low confidence in handling such threats, highlighting a significant gap between exposure and preparedness.

The results also suggest that students are motivated to improve their cybersecurity knowledge, with many expressing willingness to participate in training, workshops, and awareness programs. Analysis of open-ended responses further indicates a need for hands-on training, integration of cybersecurity topics into the curriculum, awareness campaigns, and

strengthened institutional IT infrastructure. Overall, these findings emphasize the importance of implementing multi-pronged strategies to enhance cybersecurity literacy, bridge the gap between theoretical knowledge and practical application, and promote a safer digital learning environment at Makawanpur Multiple Campus.

5. Recommendations

Based on the findings, it is recommended to organize regular hands-on workshops and practical training sessions to improve students' technical skills and confidence in handling cyber threats. Cybersecurity topics should be integrated into the curriculum across all streams of study, and offered as extra-curricular programs to ensure wider participation. Awareness campaigns, including seminars, posters, digital outreach, and classroom discussions, should be conducted to engage students and the broader campus community. Additionally, the institution should strengthen IT infrastructure, establish clear incident-reporting mechanisms, and provide technical support to model best practices and ensure timely assistance in case of cyber incidents.

References

1. Adhikari, B. P., Ale, K., & Bhusal, M. P. (2025). Understanding the key factors influencing cybersecurity practices in Nepalese organizations. *OCEM Journal of Management, Technology & Social Sciences, 4*(1), 194–208. https://doi.org/10.3126/OCEMJMTSS.V4I1.74761
2. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98,* 102003. https://doi.org/10.1016/J.COSE.2020.102003
3. Al-Sherideh, S., Maabreh, K., Maabreh, M., Al Mousa, M. R., & Asassfeh, M. (2023). Assessing the impact and effectiveness of cybersecurity measures in e-learning on students and educators: A case study. *International Journal of Advanced Computer Science and Applications, 14*(5), 2023.
4. Bhandari, B. (2025). Cybersecurity awareness amongst university students: Legal remedies and policies to mitigate risks. *Unity Journal, 6*(1), 120–135. https://doi.org/10.3126/UNITYJ.V6I1.75557
5. Bottyan, L. (2023). Cybersecurity awareness among university students. *Journal of Applied Technical and Educational Sciences, 13*(3), 363–363. https://doi.org/10.24368/JATES363
6. Dhungana, R. K., Gurung, L., & Poudyal, H. (2023). Cybersecurity challenges and awareness of the multi-generational learners in Nepal. *Journal of Cybersecurity Education, Research and Practice, 2023*(2), 5. https://doi.org/10.32727/8.2023.17
7. Du, X. (2023). *A survey of cybersecurity awareness among undergraduate students at Yunnan University of Finance and Economics in China* [Master's thesis, Chulalongkorn University]. Chula ETD.
8. Fattah, A., Wagimin, N., & Nurlia, N. (2023). Enhancing cybersecurity awareness among university students: A study on the relationship between knowledge, attitude, behavior, and training. *Jurnal Sistem Informasi (E-Journal).*
9. Gabra, A. A., Sirat, M. B., Hajar, S., & Dauda, I. B. (2020). Cyber security awareness among university students: A case study. *Science Proceedings Series, 2*(1).
10. Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346
11. Lohani, A., & Kumar, S. (2024). Impact of cyber security awareness among higher studies: Case study of Nepal. *LBEF Research Journal of Science, 6*(1).

12. Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security, 103,* 102154. https://doi.org/10.1016/j.cose.2020.102154
13. Towhidi, G., & Pridmore, J. (2023). Aligning cybersecurity in higher education with industry needs. *Journal of Information Systems Education, 34*(1).
14. Walton, S., Wheeler, P. R., Zhang, Y., & Zhao, X. (2021). An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems, 35*(1), 155–186.