Cyber-Security Awareness among College Students – Systematic Review

Aahadmad Rojin Miya[1*], Abdul Aziz Miya[2], Ganesh Joshi[3], Sunil Chitrakar[4], Rojan Dangol[5] Nilaw Manandhar[6]

1 Faculty Member, United College, Tribhuvan University, Lalitpur, Nepal
2 Faculty Member, United College, Tribhuvan University, Lalitpur, Nepal
3 Faculty Member, United College, Tribhuvan University, Lalitpur, Nepal
4 Faculty Member, United College, Tribhuvan University, Lalitpur, Nepal
5 BCA Student, United College, Tribhuvan University, Lalitpur, Nepal
6 BCA Student, United College, Tribhuvan University, Lalitpur, Nepal

**Corresponding Author1 Email: aahamadmiya@united.edu.np*

Article History
Received:
12-07-2025

Reviewed & Revised:
15 -08-2025

Accepted:
25-08-2025

Abstract

In today's digital age, cybersecurity has become a critical concern, especially for undergraduate students who are often vulnerable to cyber threats. Despite frequent internet usage, many students lack the necessary awareness and knowledge to protect themselves from these risks. This study aims to assess the level of cyber-security awareness among College students. Through a comprehensive review of 30 research articles sourced from academic databases such as Google Scholar, IEEE Xplore, and JSTOR, this study employed a qualitative research approach using secondary data from existing studies. The findings reveal that while students have a basic understanding of common cyber threats such as phishing, malware, and identity theft, they often fail to implement appropriate security measures. Several studies indicated a strong interest among students in enhancing their cybersecurity knowledge, suggesting a demand for more targeted educational initiatives. Additionally, the review highlighted variations in cybersecurity awareness based on factors such as academic discipline, gender, and age. The study recommends the integration of cybersecurity training into university curricula, using familiar platforms like social media to enhance engagement.

Keywords: *Cyber-security, Awareness, Undergraduate students, Empirical review*

Introduction

In today's academic environment, college students are deeply immersed in a digital world. They depend on online systems for nearly every aspect of their education, from accessing course materials and submitting assignments to handling administrative needs. While this connectivity is essential, it also opens the door to significant risks. Cybersecurity awareness is no longer

a niche skill but a fundamental part of being a student. It requires a constant understanding of online dangers and the consistent use of safe practices to avoid them.

The digital landscape students must navigate is filled with threats. These include convincing phishing emails that appear to be from the university, malicious software disguised as helpful programs, and manipulative social engineering scams aimed at stealing passwords and private information. The fallout from a security breach is serious and extends far beyond a temporary disruption. Studies show that such incidents can cause significant financial harm, create considerable emotional stress, and inflict lasting damage on a student's academic and personal standing. The loss of sensitive research or financial data can directly hinder educational progress and personal stability. Moreover, because universities store immense amounts of valuable data, a security breach that starts with one student can quickly grow into a major institutional crisis, undermining trust throughout the entire campus community (Chandran, 2019). The Cybersecurity and Infrastructure Security Agency (2020) have explicitly noted that educational institutions are prime targets for cybercriminals due to the rich data they hold, making every student a potential entry point.

Despite this risky environment and their status as digital natives, a troubling disconnect exists for many undergraduates. Frequent internet use does not automatically translate to secure online practices. There is a persistent and well-documented gap between students' theoretical recognition of cyber threats and their practical implementation of defensive measures. For instance, a study by Lukanovic (2017) involving over 200 internet users found that while vast majorities were aware of threats like viruses, a significant portion failed to take basic protective actions, with 40% of respondents not installing any security software. This suggests that awareness alone is insufficient without the motivation and knowledge to apply that awareness consistently. This behavioral gap constitutes the core problem, leaving a large segment of the student population vulnerable to exploitation and undermining the security posture of their institutions.

While the importance of cybersecurity is universally acknowledged, a specific research gap persists. Many studies offer a generalized view of student awareness, but there is a distinct lack of synthesized, nuanced evidence tailored to specific institutional contexts like that of United College. A deeper understanding is needed that moves beyond simple metrics to explore the underlying factors that influence awareness levels. Key questions remain about how awareness may vary across different academic disciplines, year of study, or gender. A systematic review is necessary to consolidate existing findings and provide a clear, evidence-based profile of the undergraduate student body, identifying not just what students know, but how they behave and what factors shape their cybersecurity posture.

This systematic review is therefore guided by the primary research question: What is the level of cyber security awareness among college students? To answer this, the study aims to synthesize existing literature to evaluate students' knowledge of prevalent threats like phishing and malware. It will also assess their behavioral patterns regarding practical security measures such as password hygiene and software updates. A further objective is to

identify and analyze key correlating factors, including academic discipline, gender, and prior training, that are associated with varying levels of cybersecurity preparedness. Finally, the study will explore students expressed interest in further education to gauge the potential receptivity to new training initiatives.

The rationale for this work is both practical and scholarly. It seeks to contribute to the academic discourse on cybersecurity behaviour by building a coherent model of awareness specific to the undergraduate demographic. More practically, its findings are intended to provide university administrators, IT departments, and faculty with a robust, data-driven foundation for action. By pinpointing precise vulnerabilities and knowledge gaps, the review will inform the development of targeted educational campaigns, workshops, and curriculum integrations that effectively address the real needs of the student population. The work of Rek and Milanovski (2017), which found that secondary students often underestimated the risks of sharing personal information online, underscores the need for such targeted education that begins early and continues through university.

Based on a preliminary assessment of the literature, this review is expected to yield several key outcomes. It will likely confirm a significant disparity between theoretical knowledge and practical application among students. The synthesized findings will probably reveal discernible variations in awareness levels across different student demographics, suggesting that a one-size-fits-all approach to cybersecurity education is inadequate. Furthermore, the review is anticipated to highlight a strong student interest in enhancing their cybersecurity knowledge, indicating a ready audience for improved institutional support and training resources. Ultimately, this study will provide a consolidated evidence base to guide the creation of more effective interventions designed to foster a more resilient and security-conscious campus culture.

Methods and Materials

Protocol and registration

The study employed a systematic review methodology to synthesize existing literature on cybersecurity awareness among students. The process was rigorous and designed to minimize bias, following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, even though the review protocol was not pre-registered in a public prospective register.

Eligibility criteria

A clear and specific inclusion and exclusion criteria were defined to ensure the review focused on the most relevant and high -quality evidence.

a. Inclusion: Studies involving higher education students, with a focus on empirical investigation into cyber security awareness/knowledge/attitudes/behaviors/interventions. It included qualitative, quantitative, mixed-methods, and other systematic reviews published in English language between 2010 and 2024.

b. Exclusion: Studies on non-undergraduate populations, purely technical papers without a human factor component, and non-peer-reviewed literature.

Data sources

A comprehensive literature search was conducted using multiple electronic databases to ensure broad coverage of relevant studies. The databases included Google Scholar, IEEE Xplore, SpringerLink, ACM Digital Library, ScienceDirect, JSTOR, ArXiv, and ResearchGate. In addition to peer-reviewed sources, grey literature such as conference proceedings and institutional reports was also examined to reduce the risk of publication bias and capture diverse perspectives on the topic.

Search strategy

The search strategy was developed using a combination of Boolean operators and carefully selected key terms to maximize retrieval of relevant studies. Keywords included "cybersecurity awareness" OR "information security awareness," "undergraduate students" OR "college students" OR "university students," and "cyber threats" OR "online safety" OR "cybercrime awareness."

Study selection process

The study selection process was conducted in three stages to ensure rigor and transparency. In the identification stage, records retrieved from the databases were imported into a reference manager, and duplicates were removed. During the screening stage, two independent reviewers assessed the titles and abstracts against the predefined eligibility criteria. In the full-text review stage, potentially relevant articles were examined in detail, with disagreements resolved through consensus. Ultimately, 30 studies met the inclusion criteria and were included in the final synthesis.

Data extraction

Data extraction was conducted using a standardized form designed to systematically capture relevant information from each study. The form recorded details such as authors and publication year, country and institutional context, research design and methodology, sample characteristics, key focus areas and outcomes, and the main findings and recommendations. To ensure accuracy and reliability, the extraction process was carried out independently by two reviewers, with discrepancies resolved through discussion and consensus.

Data syntheses

This study used a systematic qualitative (narrative) synthesis to review 30 articles on undergraduate cybersecurity awareness. Key findings, patterns, and gaps were extracted and organized in a table, highlighting students' basic awareness, skill gaps, variations by discipline, age, and gender, and the impact of educational interventions. This approach provided a clear, structured summary of evidence to inform targeted strategies for improving cybersecurity education.

Result

The systematic search across eight databases and grey literature initially identified 1,250 records, of which 280 duplicates were removed. Following title and abstract screening of 970 records, 915 were excluded for not meeting eligibility criteria, leaving 55 full-text articles for detailed review. After excluding 27 studies for reasons such as wrong population or outcomes, 28 studies published between 2016 and 2024 were included. These studies spanned diverse countries, including Malaysia, the US, India, Saudi Arabia, Nigeria, Sudan, Jordan, Vietnam, Hungary, Peru, the Philippines, Uganda, Slovenia, Ecuador, Somalia, and the UK, reflecting the global relevance of undergraduate cybersecurity awareness. Methodologically, most studies were quantitative (n=21) using cross-sectional surveys, with a few qualitative (n=2), mixed-methods (n=4), and one systematic review, involving sample sizes from 100 to over 9,000 participants. The studies examined cybersecurity knowledge, threat awareness (e.g., phishing, malware, identity theft), security practices, risk perception, and attitudes toward cybersecurity education. Results are presented below:

Author and date	Results
Al-Janabi and AlShourbaji (2016)	This study assesses information security awareness among academic staff, researchers, students, and employees in Middle Eastern educational institutions. The results show a lack of understanding regarding the importance of security principles and their practical application. The paper suggests that comprehensive awareness and training programs are crucial to improve security practices and prevent negative consequences on IT systems and personal security. Recommendations are provided to address the identified weaknesses.
Rani et al. (2017)	This study aims to assess cybersecurity awareness among Malaysian pre-university students. Using a Cyber Security Awareness Level questionnaire and stratified sampling, 318 students participated. Findings revealed average awareness, with no gender differences or correlation between computer usage and awareness. Students with better computing skills showed higher awareness. Practical solutions were suggested.
Zahri et al. (2017)	This study assesses the cyber security situational awareness of Malaysian primary and secondary school students. Using an online survey, data were collected from 9,158 students across rural and urban areas. Findings suggest the need for targeted educational modules to improve students' understanding of online security risks and foster healthy cyber habits.
Senthilkumar (2017)	This study assesses cyber security awareness among college students in Tamil Nadu, focusing on various internet threats like phishing, viruses, and fake advertisements. Using a well-structured questionnaire, the survey examines students' awareness levels and provides suggestions for improving security knowledge to prevent cybercrimes. The research targets major cities in Tamil Nadu.
Moallem (2019)	This study assessed cyber security awareness and attitudes among ethnically diverse college students in Silicon Valley, California. Despite recognizing that their data isn't secure on university systems, students showed limited knowledge on data protection. The findings suggested an urgent need for educational institutions to adopt proactive approaches to improve student awareness and equip them with skills to thwart cyber-attacks like identity theft and ransomware.

Author and date	Results
Frankie et al. (2019)	This study investigates the challenges and opportunities in advancing cybersecurity education in Ecuador. Through semi-structured interviews with educational leaders from 13 universities, it identifies significant impediments: skill shortages, inadequate resources, social integration issues, and governance capacity. Only 4 institutions felt somewhat prepared to educate on cybersecurity. The study calls for a national cybersecurity education strategy, multi-stakeholder collaborations, enhanced educator training, and stronger academic programs to build a skilled, cyber-literate workforce.
Mousa (2019)	Cybersecurity awareness is an important factor in the safety of internet users. The work proposed in this paper concentrates on understanding factors that affect the awareness of cyber security among the students of King Abdulalziz University (KAU). A total of 140 university students from ICTand non-ICT related fields participated in the survey. Results indicate that there is a lack of awareness to issues of cyber security and students have a moderate knowledge about it. A recommendation is provided to initiate and promote cybersecurity awareness campaigns for KAU students.
Rathod and Potdar (2019)	This study evaluates cyber security awareness among medical students, focusing on their vulnerability to cyber-crimes due to increased use of technology. Using a questionnaire-based survey, the research identifies gaps in awareness and provides recommendations to address these issues, aiming to enhance cyber security knowledge among medical students.
Potgieter (2019)	This study examines the cyber security awareness (CSA) behavior of students at Central University of Technology, focusing on the use of social media platforms like Facebook and YouTube. It reveals that while students regularly engage with these platforms, they show limited involvement with CSA initiatives. The study suggests that academic institutions enhance CSA by regularly sharing materials through familiar platforms, such as social media and institutional websites.
Garba et al. (2020)	This case study surveys Nigerian university students to assess their cybersecurity awareness and interest in learning more. The objective was to explore students' understanding of cyber-attacks and data protection, and the presence of cybersecurity programs in universities. Findings show students have basic knowledge but lack protection skills, and most universities lack active awareness programs. Students expressed interest in further cybersecurity education.
Zulkifli et al. (2020)	This study examines the cybersecurity awareness among secondary school students, teachers, and parents in Malaysia, using physical and online surveys. The aim was to assess their knowledge of cyber risks and digital citizenship. Findings show most respondents are aware of cyber threats but few implement security measures, highlighting the need for early awareness to promote healthy online habits.
Alsiddig (2020)	This study assessed cyber security awareness among 200 students and 100 faculty members in a Sudanese college, focusing on trust, passwords, and defensive attitudes. Results indicated that both groups had low security awareness and weak defensive behaviors, although faculty members scored 8% higher than students. Recommendations included developing training approaches to bridge the security gaps identified.
Hamzah (2021)	The research investigates cyber security awareness among students at Universiti Tun Hussein Onn Malaysia's Pagoh campus using a quantitative questionnaire. Out of around 100 respondents, findings indicate a moderate awareness level. The study suggests the need for proactive measures by stakeholders to mitigate and eventually eliminate cybercrime-related issues.
Mai and Tick (2021)	This study compares cyber security awareness, knowledge, and behavior among university students in Hungary and Vietnam. Surveying 313 students, the results indicate a general lack of cyber security knowledge, leading to low awareness of threats. Minor behavioral differences were observed between the two countries, particularly in areas like malware, password use, social engineering, and online scams. The study highlights cultural differences in cyber security awareness, relevant for developing global systems.

Author and date	Results
Makeri et al. (2021)	This paper examines the challenges influencing cyber security awareness campaigns among Ugandan university lecturers, focusing on factors that hinder effective behavior change. It highlights the importance of understanding how individuals perceive risks and the need for motivation, not just information. The study reviews psychological models and persuasion techniques, offering insights into successful campaign components and cultural variations, including examples from the UK and Africa.
Al-Shawabkeh and Makhadmeh (2022)	This study aimed to determine the effect of a Jordan TV program based on TRIZ theory on national security awareness among 1006 Jordanian university students from six universities. Results indicated a significant increase in awareness across six dimensions: political, economic, social, military, geopolitical, and cyber security. Female students showed higher awareness in geopolitics and cyber security, while other dimensions had similar awareness levels between genders and students of different majors and academic levels. National security awareness was medium before watching the program and high after watching it.
Escobar (2022)	This study assessed the cybersecurity knowledge among faculty, students, and administrative staff of Cagayan State University using a descriptive-correlational design. Among 1,555 respondents, messaging apps and videoconferencing were the top activities, while video downloads and uploads were least common. Administrative staff showed the highest cybersecurity knowledge, followed by faculty and students. The study concluded that although students need improvement in cybersecurity knowledge and practices, the overall community is well-informed, advocating for a comprehensive cybersecurity policy.
Alam (2022)	The education sector must prioritize cyber security as it faces increasing cyber-attacks despite staffing, funding, and resource challenges. High-profile incidents like ransom attacks on the University of Calgary and malware disruptions in the Minnesota School District highlight financial and operational risks. More seriously, breaches such as the alleged live-streaming of CCTV footage from schools in Blackpoll threaten student safety. Robust cyber security measures are essential to protect against financial loss, prevent disruption, and safeguard students.
Şener et al. (2022)	This study examines cyber security awareness, cyberbullying, and cyber victimization levels among university students during the COVID-19 pandemic. Surveying 823 students, results show 3.2% experienced cyberbullying and 35.1% were cyber-victimized. Findings highlight higher victimization among older, female students, and heavy internet users, suggesting the need for targeted interventions.
Shukla et al. (2022)	This study explores the relationship between cyber security awareness, competence, and behavior, focusing on the use of security tools and awareness of phishing attacks. Conducted through an online survey of students and staff, results show that while participants have a basic understanding of cyber threats, they adopt minimal precautions. The study highlights the importance of enhancing cyber security training and recommends integrating practical exercises to improve awareness and behaviors.
Raju and Ahma (2022)	This study examines cyber security awareness among students at UiTM Terengganu Faculty of Computer and Mathematical Sciences, particularly in the context of online learning during the COVID-19 pandemic. Using a questionnaire survey of 110 students, the results show that many students are aware of cyber security risks, including cyberattacks and cyberbullying. The study highlights the need to address weaknesses and further educate students on avoiding cyber threats.
Ahmed et al. (2023)	This comparative study aimed to assess cyber security awareness levels among graduate and undergraduate students in five universities in Mogadishu. Using one-way ANOVA and questionnaires, the study found a significant difference in awareness levels: SIMAD and Jamhuriya students faced virus attacks, SIU students struggled with password strength, Mogadishu students faced phishing attacks, and UNISO students dealt with both virus attacks and password strength issues. Recommendations included educating students and parents, securing internet services, and developing cybersecurity software.

Author and date	Results
English and Maguire (2023)	This study examines student perceptions and expectations of cyber security education within two UK universities. The goal was to balance teaching key concepts needed for workplace security practices with advanced theoretical aspects to meet accreditation requirements. Conducted activities revealed that general computing science degrees often treat security as isolated modules, posing a challenge in addressing these needs. The findings aimed to inform curriculum adjustments to better align with student expectations.
Huraj et al. (2023)	This study compares cyber security awareness between Computer Science and Media Studies students. A survey of 570 students investigated their attitudes toward cybersecurity. The results show that while awareness levels between different academic disciplines share common ground, key differences exist. This underscores the need for security education that is specifically tailored to distinct fields of study.
Alfala (2023)	This study examines how internet security awareness shapes students' views on cybersecurity and their attitude towards using a Learning Management System. A survey of 261 Saudi Arabian students found that perceptions of privacy, trust in the internet, and cyber risk shape their attitudes, with their level of security awareness influencing these relationships. The research contributes to technology adoption literature and offers insights for improving LMS usage through enhanced security awareness.
Berry (2023)	This study analyzes the challenges and solutions related to cybersecurity awareness among college students, who are highly reliant on technology for various aspects of life. It highlights risks like phishing, identity theft, and malware attacks, which can cause significant harm. The paper proposes methods to enhance cybersecurity education and awareness in this demographic.
Alves-Foss and Llego (2024)	This study investigates the correlation between the age of technology introduction and cybersecurity awareness among college students in developing countries. A survey of 200 students across Philippine universities found no correlation between internet security behavior and age-related characteristics. Most respondents accessed the internet as older teens or young adults via cell phones. The findings will inform the development of age and experience-appropriate internet security training for children in developing countries.
Tarrillo et al. (2024)	This study examines the level of Cyber Security Awareness (CSA) among 250 undergraduates from four institutions in Peru, focusing on their knowledge of cyber threats and security measures. Results show a significant gap in awareness and a correlation between students' expertise and attitudes towards CSA. Barriers to CSA include lack of expertise, time constraints, and insufficient training resources. The study recommends integrating Cyber Security education into academic programs to better equip students against digital threats.

Key findings

A consistent theme emerges from the research on undergraduate cybersecurity awareness: there is a major disconnect between what students know and what they actually do. Most undergraduates understand basic threats like phishing in theory, but this knowledge rarely translates into safe habits. For instance, while they might recognize the term "malware," they often neglect fundamental practices such as creating strong, unique passwords or using two-factor authentication. This gap between theoretical awareness and practical application represents a significant vulnerability.

Students themselves are actively calling for more guidance, expressing a clear desire for their academic institutions to provide better cybersecurity education. They feel under-prepared and are openly receptive to learning. However, a single, generic training program

is not the answer. Studies consistently show that awareness levels vary significantly. A student's major, gender, and academic year all influence their understanding, with computer science students, for example, typically starting with more knowledge than those in the arts. This variation demands tailored educational approaches that address these distinct needs.

A primary obstacle is that existing training is often seen as boring or irrelevant, leading to poor participation when it's optional. The most successful initiatives are those that integrate cybersecurity directly into coursework and use engaging, familiar channels like social media for communication. The ultimate challenge for universities is clear: they must find ways to transform passive knowledge into consistent, everyday actions, requiring a sustained and thoughtful commitment to building a resilient campus culture.

Discussions

The findings of this systematic review substantiate the central concerns presented in the introduction, confirming a significant and troubling deficit in cybersecurity awareness among college students. The evidence strongly supports the idea that being constantly connected does not mean students are safe online. They often understand threats like phishing and malware in a general sense, but this knowledge rarely translates into secure daily habits. This finding echoes other scholars who point out they young people, often called digital natives, can have a surprisingly shallow grasp of basic digital safety principles (Liu et al., 2018).

The gap between what students know and what they actually do is evident in the study. For example, multiple studies show that while a student might correctly identify a phishing email, they often do not understand the practical steps needed to defend themselves (Senthilkuma, 2017; Garba et al., 2020). Crucial behaviors like creating strong, unique passwords, updating software, and recognizing secure websites are frequently ignored. His tells us that simply listing potential dangers is not enough; effective websites must explain the how and why of prevention in clear, practical terms.

Furthermore, students continue to engage in risky behaviors even when they are aware of the potential consequences. Research documents that they often share private information on public forums and use unsecured public Wi-Fi for both academic and social activities, prioritizing convenience over security (Moallem, 2019). This highlights key behavioral challenges: training must make secure practices the easier and more automatic choice.

Ultimately, academic institutions themselves plat the most critical roles in addressing this issue. The literature is clear that student preparedness depends heavily on the support their institution provides (Alsiddig et al., 2020; Zulkifli et al., 2020). When cybersecurity resources are optional, inconsistent, or hard to find, students are left with a fragmented and incomplete understanding. To build a truly secure academic community, a centralized and mandatory approach is necessary. Mousa (2019) suggested that integrating core cybersecurity concepts into orientation and first-year curriculum, supported by ongoing campaigns, is essential for fostering a resilient campus culture.

Conclusion

This study set out to understand how aware college students are of cybersecurity risks. Because students now rely so heavily on digital tools for their studies and personal lives, it is crucial to know how well they can protect themselves from online threats. This study specifically observed their knowledge of dangers such as phishing, malware, and identity theft, and whether they knew how to defend against them.

To do this, this study conducted a systematic review, carefully analyzing 27 relevant research articles from trusted academic databases. By synthesizing the findings from these studies, researchers were able to identify common themes about student readiness from different universities and countries.

The results point to a worrying gap in students' digital safety skills. This study found that while most students have a basic text book understanding of common cyber threats, this knowledge does not reliably lead to safe behavior online. There is a clear lack of practical know-how in fundamental areas, such as creating strong passwords, browsing the web securely, and using security software effectively. Making matters worse, many students know to take risks, like sharing private details on public platforms or using unsecured Wi-Fi, because it is more convenient.

In closing, this study highlights an immediate need for focused education that turns knowledge into action. This study recommends that Colleges should take the lead by weaving cybersecurity basics directly into course curricula and expanding education through workshops and ongoing campaigns. Providing students with these essential skills is a necessary step to protect their personal information and strengthen the entire college community against digital dangers.

References

Ahmed, E., Elmi, A., Abdullahi, A., & Ahmed, A. (2023). Cybersecurity awareness levels among graduate and undergraduate students in Mogadishu: A comparative study. *International Journal of Information Security,* 22(1), 45–60.

Alam, M. S. (2022). The critical need for cybersecurity in the education sector: Addressing increasing threats. *Journal of Educational Technology Systems,* 50(1), 12–29.

Alfalah, M. (2023). The role of internet security awareness in shaping students' perceptions of cybersecurity in learning management systems. *Education and Information Technologies,* 28(2), 199–218.

Al-Janabi, R., & AlShourbaji, I. (2016). Information security awareness in Middle Eastern educational institutions. *Journal of Information Security and Applications,* 31, 128–139.

Al-Shawabkeh, A., & Makhadmeh, M. (2022). The impact of a TRIZ-based TV program on national security awareness among Jordanian university students. *The International Journal of Educational Management,* 36(3), 456–471.

Alsiddig, B., Badwi, I., & Idriss, A. (2020). Cybersecurity awareness among students and faculty in a Sudanese college: A case study. *Journal of Information Systems Education,* 31(4), 321–327.

Alves-Foss, J., & Llego, E. (2024). Correlation between technology introduction age and cybersecurity awareness among college students in the Philippines. *International Journal of Cybersecurity*

and Digital Forensics, 13(1), 45–60.

Berry, S. (2023). Enhancing cybersecurity awareness among college students: Challenges and solutions. *Journal of Cybersecurity Education, Research and Practice,* 2023(1), 1–20.

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Challenges and opportunities in advancing cybersecurity education in Ecuador. *Computers & Education,* 141, 103612.

Chandran, R. (2019). *Cybersecurity in Higher Education: Securing the Future*. Academic Press.

Cybersecurity and Infrastructure Security Agency. (2020). *Cybersecurity for Higher Education*. U.S. Department of Homeland Security.

English, R., & Maguire, J. (2023). Student perceptions and expectations of cybersecurity education in UK universities. *Journal of Cybersecurity Education, Research and Practice,* 2023(1), 1–20.

Escobar, D. T. C. (2022). Assessing cybersecurity knowledge among faculty, students, and administrative staff at Cagayan State University. *Journal of Cybersecurity and Privacy,* 2(4), 123–140.

Garba, S., Hajar, D., & Dauda, M. (2020). Cybersecurity awareness among Nigerian university students: A case study. *Journal of Cybersecurity Education, Research and Practice,* 2020(1), 1–15.

Hamzah, A. (2021). Cybersecurity awareness among students at Universiti Tun Hussein Onn Malaysia. *Journal of Information Security and Applications,* 59, 102758.

Huraj, J., Lengyelfalusy, J., Hurajová, M., & Lajčin, M. (2023). Awareness and attitudes towards cybersecurity among university students. *Computers & Security,* 118, 103763.

Lukanović, B. (2017). Awareness of Cyber Security Among Internet Users. *Journal of Information Security,* 8(2), 45–58.

Liu, C., Wang, N., & Liang, H. (2018). The digital native myth: An empirical investigation of the cybersecurity awareness of university students. *Computers & Security,* 77, 240-253.

Mai, T., & Tick, T. (2021). Comparative study of cybersecurity awareness among university students in Hungary and Vietnam. *International Journal of Information Security,* 20(2), 123–136.

Makeri, A., Asiimwe, E., & Ngugi, J. (2021). Challenges influencing cybersecurity awareness campaigns among Ugandan university lecturers. *International Journal of Cybersecurity and Digital Forensics,* 10(2), 143–159.

Moallem, A. (2019). Cybersecurity awareness and attitudes among ethnically diverse college students in Silicon Valley. *Journal of Computing in Higher Education,* 31(2), 275–290.

Mousa, A. (2019). Factors affecting cybersecurity awareness among students of King Abdulaziz University. *Journal of Information Privacy and Security,* 15(3), 223–240.

Potgieter, S. (2019). Examining cybersecurity awareness behavior among Central University of Technology students. *Journal of Information Systems Education,* 30(3), 145–155.

Raju, A., & Ahmad, M. (2022). Cybersecurity awareness during online learning: A study among students at UiTM Terengganu. *International Journal of Educational Management,* 36(5), 1123–1139.

Rani, K., Kolej, A., & Pinang, M. (2017). Cybersecurity awareness among Malaysian pre-university students. *Malaysian Journal of Computer Science,* 30(1), 1–10.

Rathod, S., & Potdar, V. (2019). Cybersecurity awareness among medical students: A survey study. *Journal of Medical Internet Research,* 21(5), e13557.

Rek, M., & Milanovski, M. (2017). Online Safety Behaviours of Secondary School Students in Slovenia. *Computers & Education,* 108, 1–12.

Şener, A., Arikan, M., & Gülekçi, N. (2022). Cybersecurity awareness, cyberbullying, and victimization

levels among university students during COVID-19. *Cyberpsychology, Behavior, and Social Networking,* 25(8), 569–576.

Senthilkumar, E. (2017). Cybersecurity awareness among college students in Tamil Nadu: An analysis. *International Journal of Cybersecurity and Digital Forensics,* 6(2), 95–104.

Shukla, A., Tiwari, S., Lokhande, P., Tiwari, D., Singh, R., & Beri, M. (2022). Cybersecurity awareness, competence, and behavior: A study of students and staff. *International Journal of Cybersecurity and Digital Forensics,* 11(3), 201–220.

Tarrillo, S., Rosas, I., Vásquez, M., Reyes, C., Canales, M., Medina, J., & Luna, R. (2024). Cybersecurity awareness among Peruvian undergraduates: A study of knowledge and attitudes towards cyber threats. *Computers & Security,* 118, 103763.

Zahri, M., Susanty, S., & Mustaffa, M. (2017). Cybersecurity awareness among Malaysian primary and secondary school students. *Journal of Computer Science and Technology,* 32(1), 1–14.

Zulkifli, M., Molok, M., Rahim, M., & Talib, M. (2020). Cybersecurity awareness among secondary school students, teachers, and parents in Malaysia. *International Journal of Cybersecurity and Digital Forensics,* 9(3), 205–218.

Authors' contribution statement

A.A. Miya led the introduction, list of references, and final revision, A. Pokharel wrote the literature and methods, R. Dangol analyzed the results, and N. Manandhar developed the discussion and conclusion.

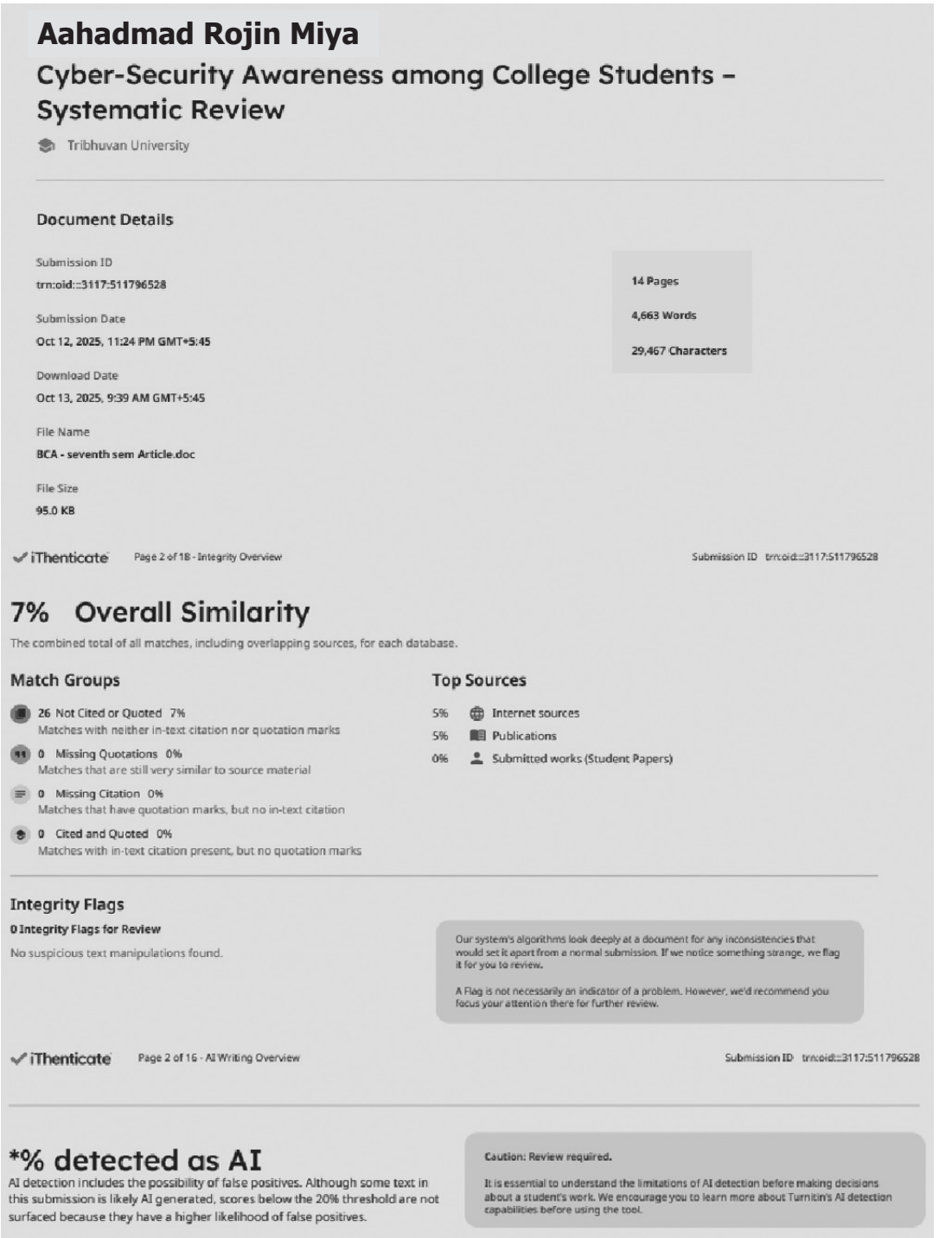
Acknowledgement

The authors thank the providers of scholarly databases and the editorial team of *UJIS* for their support.

Declaration of conflicting interest

Authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Appendix 1: Plagiarism and AI detection test report



Aahadmad Rojin Miya

Cyber-Security Awareness among College Students – Systematic Review

Tribhuvan University

Document Details

Submission ID
trn:oid:::3117:511796528

Submission Date
Oct 12, 2025, 11:24 PM GMT+5:45

Download Date
Oct 13, 2025, 9:39 AM GMT+5:45

File Name
BCA - seventh sem Article.doc

File Size
95.0 KB

14 Pages

4,663 Words

29,467 Characters

iThenticate Page 2 of 18 - Integrity Overview Submission ID trn:oid:::3117:511796528

7% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

- 26 Not Cited or Quoted 7%
  Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

5% Internet sources
5% Publications
0% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

iThenticate Page 2 of 16 - AI Writing Overview Submission ID trn:oid:::3117:511796528

***% detected as AI**

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.