The OCEM Journal of
Management, Technology & Social Sciences

Received: Aug 02, 2025 | Revised: Sep 05, 2025 | Accepted: Sep 10, 2025 | Published: Jan 10, 2026

DOI:10.3126/ocemjmtss.v5i1.89684 **Paper Type: Research Article**

Assessing the Cybersecurity Literacy Proficiency among Bachelor's Degree Students in Nepal

Basanta Prasad Adhikari[1]*, Amrit Acharya[2], Arbin Chhatkuli[2], Ankur Ghimire[2], Lalita Poudel[2]
[1]Faculty of Research, Oxford College of Engineering and Management, Nepal
[2]BCA Scholar, Oxford College of Engineering and Management, Nepal
*Correspondence email: adhikaribasantaprasad@gmail.com

Abstract

Volume 5, Issue 1

ISSN Print:2705-4845

ISSN Online:2705-4845

As Nepal's higher education system is being shifting toward digitalization, the importance of cybersecurity literacy among the bachelor students has never been greater. With growing threats and risks like phishing, scams and data breaches, it is essential to understand how well students are prepared to protect themselves in this digitalized environment. Improving the cybersecurity literacy in higher education can play very important role in preparing students for a secure digital future and reduce the unwanted exposure to digital threats, scams and risks. Our study aims to examine the cybersecurity awareness level among bachelor-level students in Nepal. Understanding their knowledge, attitude, and day-to-day practices is our main aim. Our study employed a quantitative survey method to collect data from two hundred and ten (N = 221) samples. The survey method was used to gather students' opinions and experiences regarding digital threats, their efforts to mitigate these threats, and the impact of cybersecurity education in their day to day online presence.

The descriptive statistics was used to analyse the collected data, along with the application of a binary logistic regression model. The findings reveal that Nepalese bachelor level students have poor awareness about cybersecurity threats which show a noticeable gap in cybersecurity education, spreading vulnerabilities and limited impact of current training initiative. The result further highlights that there was no association between cybersecurity awareness level and gender. The results importantly that students are familiar with common cyberattacks, understand how they manage the risks, and the effectiveness of current cybersecurity education efforts. By examining key factors that influence cybersecurity awareness, it offers benefits to educational, social and technical institutions, policymakers, and cybersecurity professionals to understand the current level cybersecurity awareness of youths.

Keywords: *bachelor's degree students, cyber awareness, cybersecurity literacy, digital threats, digitalization in Nepal*

How to cite this paper:
Adhikari, B.P., Acharya, A., Chhatkuli, A., Ghimire, A., & Poudel, L. (2026). Assessing the Cybersecurity Literacy Proficiency among Bachelor's Degree Students in Nepal. *The OCEM Journal of Management, Technology & Social Sciences, 5*(1), 23-36.

Introduction

The COVID-19 epidemic necessitated a swift global transition to online learning, notably in developing countires, to ensure educational continuity. However, this swift change often overlooks security, leaving e-learning platforms vulnerable to different risks, which are vulnerable to technical, management, and user-related issues, including poor design, insufficient authentication, and data integrity problems. Malicious actors can exploit these weaknesses to gain unauthorized access to systems, modify data and initiate attacks (Djeki, Degila & Alhassan, 2024).

Even while developers and system administrators should follow security best practices, the user is often the weakest link. User behaviour, whether deliberate or inadvertent, can undermine system security and result in data breaches. Therefore, students must be aware of and adhere to security rules closely (Djeki et al., 2024). Because of these platform and user weaknesses, it is essential to utilize every feasible security precaution. To achieve this well in developing countries, you need to be aware of the specific tools, platforms, and, most crucially, the cybersecurity knowledge and behaviuor of the pupils. Our paper aims to identify the security vulnerabilities of prevalent e-learning platforms and assess the cybersecurity awareness and responsibilities of students in developing countries. The study evaluated the current literature, elaborate on its research methodologies, and scrutinise survey data to fulfil its objectives.

Cybersecurity is the process, method, and technology that keeps devices, networks, and hardware safe from digital attacks and risks (Indian Emblem Government of India Press Information Bureau, 2017). It is the act of keeping systems, networks, and applications safe from digital threats. Cyberattacks typically aim to access, modify, or delete sensitive data; extort money from users by threatening to disclose it, and disrupt normal corporate operations (Ahmed & Ahmed, 2019).

Cybersecurity is now a crucial skill for everyone who uses the internet, especially students, who spend a significant amount of time online learning (Ahmed & Ahmed, 2019). The more people utilise digital gadgets and online services, the more likely they are to become victims of cybercrime, such as phishing, hacking, and data breaches. Teenagers are more likely to be the targets of cyberattacks; therefore, they need to be aware of cybersecurity to ensure whether their online activities are safe (Indian Emblem Government of India Press Information Bureau, 2017). The education system in Nepal is slowly moving towards digital platforms. Increasingly, students are taking online classes, completing digital assignments, and conducting research on the internet. However, many students lack sufficient knowledge about cybersecurity, making them vulnerable to cyberattacks. They might not know how to keep their personal information safe, spot cyber risks, or utilise digital services responsibly. This lack of cybersecurity knowledge can put pupils at risk of online attacks, scams, data leaks, and cyberbullying. People are concerned that pupils may accidentally share private information, use weak passwords, and click on unknown or harmful websites (Giri, 2021).

Most educational institutions are trying to improve their IT infrastructure, but they often overlook the importance of training and informing students. Even intelligent and tech-savvy students can be targeted by cyberattacks if they do not understand how to protect themselves. Therefore, it is essential to determine the current level of cybersecurity knowledge among bachelor's students in Nepal, allowing them to identify gaps and develop effective educational and awareness initiatives (Giri, 2021).

Educational institutions are at risk of several serious problems if their students and staff lack sufficient knowledge about cybersecurity. These include a greater risk of cybercrime and data breaches, which can compromise private information. Basit et al. (2025) stated that a lack of awareness also compromises the integrity of education, as more cyber cheating and misuse of digital tools are typically associated with a lack of sufficient knowledge or understanding. They also stated that insufficient cybersecurity policies can compromise students privacy and online reputation, potentially making them less confident about using digital platforms for both school and personal purposes (Basnet et al., 2025).

Basit, Waheed & Oguntayo (2025) corroborated the findings of Schrieks et al. (2021), highlighting that inadequate cybersecurity practices are significant as they indicate the prevailing degree of cybersecurity awareness and literacy among undergraduate students. Schrieks et al. (2021), further noted that with the rise of internet use in education, it is crucial to comprehend how students navigate their online presence. The results can be utilized by schools, institutions, policymakers, training programs, and awareness campaigns to increase public awareness of cybersecurity. This study also inspired bachelor's-level students to utilise the internet properly and make the online academic world safer. Our study aims to assess and understand the level of cybersecurity literacy among bachelor's degree students in Nepal. Our research aims to identify the domains in which they exhibit a lack of awareness and understanding of cybersecurity.

Research questions

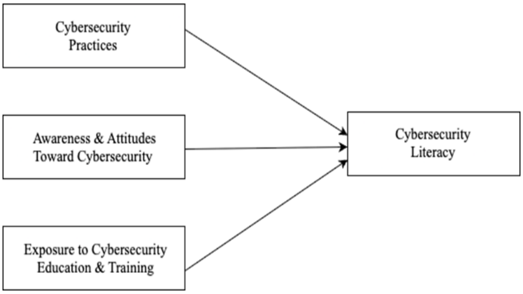
What do bachelor's degree students already know about basic cybersecurity practices?

What do bachelor's degree students already know about standard cybersecurity practices?

What do bachelor's degree students think about the hazards of cybersecurity attacks, and how do they feel about their own online safety?

What is the relationship between formal cybersecurity education and the use of secure online practices among bachelor's degree students?

Conceptual Framework


Cybersecurity Practices
Awareness & Attitudes Toward Cybersecurity
Exposure to Cybersecurity Education & Training
Cybersecurity Literacy

Hypothesis

H$_1$: Bachelor's degree students have an incomplete understanding of cybersecurity practices.

H$_2$: Students show low awareness and an indifferent attitude towards cybersecurity threats.

H$_3$: Formal cybersecurity education increases student awareness and adoption of secure online behaviours.

Theoretical Foundation of this Study

The research focuses on two principal theories: the Protection Motivation Theory (PMT) and a contemporary theory known as TAM. PMT, proposed by Roger (1962) is the response of humans when they encounter messages that induce anxiety and drive them to adopt defensive actions, as recommanded by Rogers (1962). The theory posits that an individual's drive for self-protection is dependent on two variables. When evaluating a threat, we began by determining its severity and potential impact. The coping assessment is another factor to consider. It examines whether people trust their protective measures and are confident in their effectiveness and conceived the idea for TAM in 1986. It examines how people learn about and utilize new technologies. Two of these are the most important: how well technology seems to aid individuals with their tasks and how easy it is to use. These theories elucidate the influence of cybersecurity literacy on individuals and organisations in identifying online threats and selecting secure technologies and behaviours.

The Theory of Planned Behaviour (TPB), introduced by Ajzen (1991), is important to this research. This theory posits that an individual's intention to act is dependent on three factors: their attitude towards the activity, subjective norms and perceived social pressure, and perceived behavioral control. People are more likely to behave positively if they have an optimistic attitude, trust others, and take action. Learning about cybersecurity can help people develop responsible online habits, feel supported by their community, and become more confident in their ability to protect themselves.

This study utilises Everett (Rogers;1962) Diffusion of Innovation Theory to elucidate the mechanisms by which ideas disseminate throughout organisations and communities. This idea posits that humans advance through stages: initially hearing about something novel, developing an interest, assessing its value, experimenting with it, and ultimately adopting it if it demonstrates efficacy. The rate at which this transpires is dependent on individuals' receptiveness to change, the responses of nearby individuals, and the novelty of the new object. Constructivist Learning Theory posits that individuals learn most effectively by assimilating new information into their pre-existing knowledge through experience, reflection, and communication. Cybersecurity training and hands-on experience help individuals learn and adopt safe practices, which in turn increase their awareness of cybersecurity issues.

International context

Low Awareness: Multiple studies, including one conducted in New Zealand (Tirumala, Deakin & Stannard, 2016) and another in the Kyrgyz Republic (Ismailova & Muhametjanova, 2016), indicate that students generally possess inadequate cybersecurity knowledge and lack awareness of prevalent cyber threats and their own vulnerabilities.

Different Levels of Knowledge: A US study (Sarathchandra, Aladag & O'Leary, 2016) found that more than 80% of students understood the meaning of fundamental cybersecurity terms. However, their overall knowledge and behaviuor were different depending on factors such as their age, gender, and internet habits.

The Discrepancy Between Awareness and Action: Studies from several locations reveal a prevalent paradox: despite students' comprehension of cyber risks, they frequently fail to implement precautionary measures. For instance, a study in Saudi Arabia (Aljohni et al., 2021) found that students in ICT disciplines were more informed; however, an American study (Althobaiti, 2021) demonstrated that even IT professionals could fall victim to phishing attempts. This pattern is also observed in a survey of students from Israel, Slovenia, Poland, and Turkey (Zwilling et al., 2022), which found that users were typically informed but did not take any action to protect themselves.

Risk-Taking Habits: Studies show that many students fail to update their devices or use antivirus software, and others find it annoying to create strong passwords or use public Wi-Fi without a VPN (Alharbi & Tassaddiq, 2021).

Influence of Gender and Geography: Certain research identified variations in awareness contingent upon demographic factors. A study conducted in Saudi Arabia indicated that female students demonstrated a marginally elevated degree of anxiety (Aljohni et al., 2021), whilst a Nigerian study revealed that female students were more prone to being victims of cyberattacks (Garba, Mohammed & Yakubu, 2020).

Concentrate on the African Nation

Numerous studies conducted in Africa reflect similar global patterns. Studies conducted in South Africa, Nigeria, and Zimbabwe have consistently revealed that pupils possess an inadequate understanding and lack the necessary abilities to address cyber dangers, despite the increasing frequency of cybercrime. The switch to online learning during the COVID-19 pandemic highlighted these weaknesses in students and instructors even more (Elradi et al., 2020; Moyo et al., 2022).

Concentrate on African Nations

Numerous studies conducted in Africa reflect similar global patterns. Studies conducted in South Africa, Nigeria, and Zimbabwe have consistently revealed that pupils possess an inadequate understanding and lack the necessary abilities to address cyber dangers, despite the increasing frequency of cybercrime. The switch to online learning during the COVID-19 pandemic highlighted these weaknesses in students and instructors even more (Elradi et al., 2020; Moyo et al., 2022).

Table 1. The summary of the previous study on Evaluating the Level of Cybersecurity Literacy Among Bachelor's Degree Students in Nepal

Authors and years	**Title of Article**	***Source of Article***	**Objective**	**Key Results**	**Research gaps**
Lohani and Kumar (2024)	Impact of Cyber Security Awareness Among Higher Studies: Case Study of Nepal	*LBEF Research Journal of Science and Technology and Management*	To analyze how much students, teachers, and university staff in Nepal are aware of cybersecurity	The results reveal the current level of cybersecurity practices, knowledge, and awareness among faculty, administrators, and students in Nepalese universities.	There is a lack of research on cybersecurity in Nepal's universities, particularly regarding the views of teachers and staff, the evolution of awareness over time, and the effectiveness of current training programs.
Bhandari (2025).	Cybersecurity Awareness amongst University Students: Legal Remedies and Policies to Mitigate Risks	*Unity Journal*	To analyze the level of knowledge among university students in Nepal regarding cybersecurity threats, including hacking and phishing.	The study found that while 67.2% of students were familiar with the term 'hacking', only 46.9% were aware of Nepal's cybersecurity laws, revealing a significant gap in both legal and practical knowledge of cybersecurity.	There is a lack of research on how well university students in Nepal understand cybersecurity threats and laws, resulting in a knowledge gap about their ability to manage digital risks.
Zwilling et al. (2022)	Cybersecurity awareness, knowledge, and behavior: A comparative study	*Journal of Computer Information Systems*	This study examines the relationship between cybersecurity awareness, knowledge, and behavior, particularly the use of protection tools, across individuals in four countries, and provides recommendations for effective cybersecurity training programs.	This study found that while internet users across four countries have good cyber threat awareness and knowledge, they tend to use only basic protection tools, with notable differences in behavior and awareness patterns between countries.	There is a limited understanding of why individuals, despite being aware of cyber threats, fail to adopt strong protective behaviors and how these patterns vary across different countries.
Chandarman and Van Nieker (2017)	Students' cybersecurity awareness at a private tertiary educational institution	*The African Journal of Information and Communication*	This study aims to investigate the level of cybersecurity awareness among students at a private tertiary institution in South Africa.	The study found that students often overestimate their cybersecurity skills, but their actual knowledge and behavior do not match, making them more vulnerable to cyberattacks.	There is limited research on the mismatch between students perceived and actual cybersecurity knowledge and behavior, particularly within private tertiary institutions in South Africa, which makes it challenging to design targeted awareness programs.
Garba, Siraj, and Othman (2022).	An assessment of the cybersecurity awareness level among	*International Journal of Electrical and Computer Engineering (IJECE)*	The objective of this study is to define the level of awareness in Cybersecurity among students in Northeastern Nigeria	The study shows that most students possess a basic understanding of cybersecurity fundamentals, particularly regarding internet banking, but have only a neutral understanding of concepts such as internet addiction, cyberbullying, and online protection.	The study lacks a comprehensive analysis across demographics, behavioral executions, longitudinal changes, and influencing factors, limiting its depth and generalizability in assessing awareness of cybersecurity.
Szumski (2018)	Cybersecurity best practices among Polish students	*Procedia Computer Science*	The objective of this study is to evaluate students' cybersecurity knowledge and behavioral patterns, with a particular focus on the sources of information and password protection practices.	The study found that students primarily rely on the internet and peers for cybersecurity knowledge, resulting in poor behavioral patterns, while practical training and institutional support are often undermined.	The absence of comprehensive, scientifically supported frameworks for assessing and raising security awareness that take into account the changing nature of cyberthreats and the various demands of various groups

Alzubaidi (2021)	Measuring the level of cybersecurity awareness for cybercrime in Saudi Arabia	*Heliyon*	To get the current level of cybersecurity awareness in Saudi Arabia through an internet questionnaire focusing on knowledge, practices, and incident reporting.	This study reveals a lack of cybersecurity awareness among participants, with 51% using personal information in passwords, 32.5% being unaware of phishing attacks, and only 29.2% report having been victims of cybercrimes.	The research gap lies in the lack of analysis on demographic factors and the effectiveness of existing cybersecurity awareness programs.
Yadav (2024)	A study on the adequacy and appropriateness of computer science curricula in Nepali secondary schools	*Doctoral dissertation, Tribhuvan University, Kathmandu*	To investigate the design and delivery of the current Computer Science (CS) curriculum for Grades 9 and 10 in Nepal.	The CS curriculum includes basic programming (HTML, CSS, QBasic, C) and database (MS Access).	More practical learning and teacher support are required.
Hong et al., (2023)	The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates.	*Education and information technologies,*	To understand what affects Internet Security Awareness in people.	This means that social and work environments can significantly influence a person's cybersecurity awareness in various ways.	More research is needed to understand how the work environment shapes behavior over time.
Lund, Anderson, Roeschley (2025)	Understanding the relationship between personal data privacy literacy and data privacy information sharing by university students.	*Journal of Information Science*	To explore how personal data privacy literacy affects students' abilities to describe responsible privacy behaviours and influence peer advice.	Survey-based study using statistical analyses (Shannon's Diversity Index, permutation analysis, chi-square tests).	High-literacy individuals display a broader range of protective behaviours (MFA, VPN, phishing awareness); low-literacy individuals rely on basic measures. High literacy correlates with greater diversity in privacy advice.
Gupta and Misra (2025)	The Impact of Data-Driven Approaches on Cyber Security Awareness in Nepal's Digital Landscape.	*Aadim Journal of Multidisciplinary Research Information & Technology*	To identify gaps in existing awareness, analyze successful global strategies, and recommend localized, actionable solutions for Nepal.	Personalized training and real-time threat monitoring enhance awareness. Traditional generic programs are insufficient due to a lack of personalization.	Traditional methods lack personalization and fail to leverage technology for targeted, proactive solutions; implementation is hindered by infrastructure constraints and low computer literacy.
Talpe 2023)	Cybersecurity among college students.	*Department of Computer Science (Inferred Academic Source)*	To assess the general level of information security awareness and cybersecurity precautions among college students in a regional context (Inferred Nepal/South Asia).[3]	Even with increased access to technology, users' knowledge of cybersecurity precautions and risk reduction methods has not shown significant improvement, reflecting low digital literacy.[3]	Need for research into training effectiveness and comparative studies of smartphone vs. computer security behaviors.[3]
Eliza et al. (2024)	Assessing student readiness for mobile learning from a cybersecurity perspective.	*Online Journal of Communication and Media Technologies*	To measure the level of cybersecurity awareness among students and identify topics needing improvement related to mobile learning (m-learning).	System updates were the only indicator rated "good." Other indicators of m-learning security awareness were rated "sufficient" or "poor."	No previous research has specifically measured students' holistic readiness for m-learning, considering cybersecurity awareness.
Shahbazi et al. (2025)	AI-Based Phishing Detection and Student Cybersecurity Awareness in the Digital Age.	*Special Issue: Big Data Analytics with Machine Learning for Cyber Security (Inferred MDPI Journal)* [8]	To evaluate students' awareness of phishing attempts and their perception of AI-based detection systems.	Most students are knowledgeable about phishing methods, but many fail to recognize the danger. High trust in AI detection (51.4%), but systems face accuracy/false positive issues.	Need for more representative samples, real-world evaluation of AI systems, and assessment of longer-term awareness changes.

Ahmed (2021)	Teachers' Awareness in Developing Student Cybersecurity: A Case Study.	*Turkish Journal of Computer and Mathematics Education*	To assess the level of awareness among teachers regarding their role in developing student cybersecurity competence.[6]	Identified moderate to low levels of student cyber awareness, emphasizing the necessity to integrate cyber security education directly into the curriculum, spearheaded by teachers [6]	There is a need for resources and continuous professional development for teachers to guide students in safe online practices.[6]
Nepal (2025)	The Impact of Data-Driven Approaches on Cyber Security Awareness in Nepal's Digital Landscape (Secondary thematic reference) [4]	*ResearchGate (Inferred Source)*	To describe students' cybersecurity-related experiences and challenges in Nepal.	The school's cybersecurity support system is inadequate; teachers have limited awareness and competencies to protect students.	There is an urgent need to enhance the cybersecurity awareness and skills of teachers due to the existing infrastructure's weaknesses.[4]

Summary of literature

Research conducted by Bhandari (2025), Chandarman and Van Niekerk (2017), Garba, Siraj, and Othman (2022), Szumski (2018), and Alzubaidi (2021) underscores that students possess only a fundamental comprehension of cybersecurity. Similarly, research conducted by Yadav (2024) and Szumski (2018) demonstrates that educational institutions often possess inadequate curricula regarding cybersecurity and cyber risks. Moreover, our review indicated that quantitative research methods, in conjunction with survey studies, were employed as sresearch methodologies in the examined papers. Nonetheless, the qualitative interview methodologies were the least employed in the examined studies. Our study highlights a substantial deficiency in knowledge and awareness among students, primarily attributed to inadequate research, particularly in the domain of cybersecurity in Nepal. All review studies utilised quantitative methodologies; nonetheless, reliance on a singular method fails to yield a comprehensive understanding of the subject. Consequently, a mixed-methods approach is essential since it seeks to comprehend the perspectives and ideas of students through two distinct lenses.

Gap in Research

Our study reveals that much past research had focused on what students know about cybersecurity. However, they did not delve into more detail about the various factors that influence how students actually behave and what they do. Most studies simply examine surface-level awareness and overlook the various factors that influence how students perform in real-life digital scenarios. There is a substantial deficiency of studies examining profound themes within the setting of Nepal. Another significant deficiency is the absence of longitudinal studies that monitor temporal changes. Most current research relies on singular surveys and did not adequately illustrate the changes in awareness and literacy that follow training or educational programs. There are also very few studies that examined the effectiveness of cybersecurity education and curricula. By addressing these shortcomings, future studies can provide more effective support to educational institutions, schools, and policymakers in Nepal, ultimately enhancing cybersecurity education and awareness among students.

Methodology and Materials

We employed a quantitative method to identify the issue of cybersecurity. The survey methodology has been utilised to comprehend the perspectives, notions, and experiences of undergraduate students concerning their awareness of cybersecurity. We used the survey method because it is cost-effective, requires minimal time, allows us to cover a large group of people simultaneously, and facilitates easy understanding of people's thoughts and feelings (Creswell & Plano Clark, 2018).

Choosing a Sample and Collecting Data

We first employed purposive sampling methods to select the sample population, and then we used random sampling methods to select the second group. Our sample comprises two hundred and ten (N

= 210) undergraduate students from the Chitwan and Nawalpur districts, Nepal. The survey questionnaire served as a research instrument for data collection. Our research has adhered to all ethical guidelines during the whole research process. Initially, we conducted a survey questionnaire, informed by our literature analysis, on a sample population of five as a pilot study to identify deficiencies in the research instrument (Adhikari, 2025). Following our pilot study, we were advised to modify some of the comments made by the pilot respondents. The biggest problem was the unclear wording and some instruments that could be interpreted in more than one way. Then we attempted to determine the appropriate sample population. To obtain an example, we went to different educational institutions in Chitwan and Nawalparasi, Nepal. We first contacted the head of the institution and requested permission to collect the data.

We were instructed to meet at a different educational institutions at a separate time. After the meeting, they allowed us to speak with students who were pursuing their bachelor's degrees. The next time, we visited several institutions to identify potential sample populations. Before collecting data from our sample of two hundred and fifty (N = 250) bachelor-level students, we emailed them a consent form. Only two hundred and ten (N = 210) of them sent back the consent forms. We distributed our questionnaire online to two hundred and ten (N = 210) people, but only seventy (N = 70) responded. We understand that an online survey alone would not be sufficient. We then printed out one hundred and thirty (N = 130) survey forms and administered them to the person. We cleaned our data and prepared it for analysis after collecting it from two hundred and ten (N = 210) samples.

We used SPSS to look at our data. We used descriptive statistics to analyze the data and factor reduction method to identify the Principal Components (PCs) from the survey instruments. We utilised AI templates to produce graphics, graphs, charts, and figures (Kalame, Luukkanen, & Kanninen, 2011).

At the first level of the study, descriptive statistics were used to summarize the data, including means, frequencies, percentages, and standard deviations. These descriptive data elucidate the awareness, behaviour, and habits of bachelor's degree students in Nepal.

Principal Component Analysis (PCA) was employed to identify the key elements that impact cybersecurity literacy and awareness. This technique helps condense survey items or inquiries into more manageable elements (Adhikari, 2022). We verified the data's reliability by calculating the Alpha values. The alpha values that are higher than 0.600 demonstrate that the data obtained is reliable (see Tables 2 and 4).

Results

The results of the factor reduction model indicate that the KMO value for the first and second Principal components is 0.894, suggesting the need for further data analysis. Similarly, the total variance explained by the first principal component and second principal component is 44.64% and 17.13% respectively (see Table 2).

Table 2. Values of Mean, SD, Alpha, Variance explained, and KMO

Principal components	Mean	SD	Alpha	Variance explained	KMO
Personal Cybersecurity Practices	2.227	.987	.876	44.62%	.894
Data Protection and Network Security	2.136	.712	.658	17.14%	

The results show that the mean values of both PCs do not differ significantly, indicating that respondents disclose that they were dissatisfied with the statements of they enable two-factor authentication (2FA) on all their important online accounts (e.g., email, banking, social media), they are careful about clicking links or opening attachments from unknown sources in emails or messages, they update the privacy settings on my social media profiles. They are cautious about what personal information they share online or on social media, cybersecurity practices uses weak password, they have antivirus or anti-malware software installed on my personal laptop/computer and keep it updated, we put back up important files to a secure external drive or cloud service, we avoid using public Wi-Fi networks (e.g., cafés, parks) without a VPN, ANDI consistently update the operating system and applications on their devices to the latest versions (see Table 2).

Independent t-test

Based on the provided T-test output, the results for both personal security practices and data protection and network security were not statistically significant, suggesting that there is no meaningful difference in the cybersecurity behaviours of the two groups being compared. For the personal security practices variable, the p-value of 0.342 is significant above the 0.05 significance level. For data protection and network security, the p-value is even higher at 0.403. In both cases, the 95% confidence intervals contain zero, which further confirms that any observed difference in the mean scores is likely due to chance rather than a real effect. Therefore, the data shows that both groups have similar levels of engagement in these cybersecurity habits.

Regression analysis

The Omnibus Tests of Model indicate a good fit for the data because the model's chi-square is significant [X^2 (2) = 7.033, p = .030]. Additionally, the Hosmer and Lemeshow test shows an improved fit with the regression model since the p-value is not significant [X^2 (2) = 7.047, p = .532]. The model predicts that all one hundred fourty-seven (N = 147) bachelor-level students in the study used a unique, strong password for each online account; however, it misclassifies seventy two (N = 72) students who did not use such passwords, while accurately classifying 99.3% of the students.

Table 3. Factors predicting on personal cybersecurity practices, data protection, and network security in students, using unique and strong passwords (n = 221)

							95% C.I.for EXP(B)	
Independent variables	**B**	**S.E.**	**Wald**	**df**	**Sig.**	**Exp(B)**	**Lower**	**Upper**
Personal Security Practices	-.356	.144	6.102	1	.014	.700	.528	.929
Protection and Network Security	-.146	.148	.965	1	.326	.864	.646	1.156
Constant	-.731	.147	24.906	1	.000	.481	-.731	

Overall, the correctness rate is 67%. These results suggest that the regression model generally fits the data, but the weak association between the independent and dependent variables indicates a limited relationship. The -2 Log Likelihood of 273.373 measures the model's goodness of fit, with lower values indicating a better fit. The pseudo-R-squared values, Cox & Snell R-squared (.031) and Nagelkerke R-squared (.044), estimate the proportion of variance explained; their low values indicate that the predictors have a moderate effect on the outcome.

The results show a significant negative relationship between personal cybersecurity practices and students using unique, strong passwords in their online accounts (odds = .700, B = -.356<1, p = .014). However, there is no association between data protection, network security, and students' regular use of unique and strong passwords during their online activities (p > .05) (see Table 3). The results of the factor reduction model indicate that the KMO value for the first and second principal components is 0.824, suggesting the need for further data analysis. Similarly, the total variance explained by the first principal component and second principal component is 43.42% and 17.62% respectively (see Table 3).

Table 4. Mean, SD, Alpha, Variance explained, and KMO

Principal components	**Mean**	**SD**	**Alpha**	**Variance explained**	**KMO**
University cybersecurity literacy	2.898	.872	.901	44.64%	.824
Mandatory cybersecurity education	2.277	.859	.615	13.13%	

The results of the factor reduction model show that the KMO value of the first and second principal components is 0.824, which signifies the need for further analysis of the data. Similarly, the total variance explained by the first principal component and second principal component is 44.64% and 13.13% respectively (see Table 2).

The results further indicate that respondents disclosed their opinions and experiences based on no clear idea about using unique and strong passwords while using online accounts. They disclosed that they did not know for the statements of their university provides guidelines or resources on safe online practices, they have received cybersecurity tips or awareness messages via university emails or announcements, they have practiced cybersecurity tasks during classroom or lab assignments, discussions with peers or faculty have significantly improved their cybersecurity awareness, their bachelor's degree curriculum has included dedicated modules or lessons on cybersecurity, the cybersecurity education they received was relevant to real-world threats and they have completed self-paced online courses or tutorials on cybersecurity.

Regression analysis

The Omnibus Tests of Model indicate a good fit for the data because the model's chi-square is significant [X^2 (2) = 9.008, p = .011]. Additionally, the Hosmer and Lemeshow test shows an improved fit with the regression model since the p-value is not significant [X^2 (2) = 7.590, p = .370]. The model predicts that all one hundred and fourty eight (N = 148) bachelor-level students in the study used a unique, strong password for each online account; however, it misclassifies seventy three (N = 73) students who did not use such passwords, while accurately classifying 67 % of the students.

Table 5. Factors predicting on personal cybersecurity practices, data protection, and network security in students, using unique and strong passwords (n = 221)

Independent variables							95% C.I.for EXP(B)	
	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
University cybersecurity literacy.	-.456	.159	8.264	1	.004	.634	.465	.865
Mandatory cybersecurity education	-.021	.147	.021	1	.885	.979	.733	1.306
Constant	-.744	.148	25.184	1	.000	.475		

Overall, the correctness rate is 68%. These results suggest that the regression model generally fits the data, but the weak association between the independent and dependent variables indicates a limited relationship. The -2 Log Likelihood of 271.398 measures the model's goodness of fit, with lower values indicating a better fit. The pseudo-R-squared values, Cox & Snell R-Square 4% (.043) and Nagelkerke R-Square 5.8% (.058), estimate the proportion of variance explained; their low values indicate that the predictors have a moderate effect on the outcome.

The results show a significant negative relationship between educational institutions cybersecurity literacy and students using unique, strong passwords in their online accounts (odds = .637, B = -.456 < 1, p = .004). However, there is no association between data protection, network security, and students' regular use of unique and strong passwords during their online activities (p > .05) (see Table 5).

Summary of the results

The Alpha values of the subscales (PCs) indicate that the data are pretty reliable, as evidenced by the higher Alpha scores (see Tables 2 and 4). The results demonstrate that the mean values of both PCs are not very different from each other. This means that the student who answered were not aggred with the students, as shown by the mean values of the first and second PCs, which are 2.227 and 2.136, respectively, both below the average value (3) (see Table 2). The findings indicate that respondents demonstrated doubt and a lack of clarity regarding the utilisation of unique and robust passwords for online accounts, as evidenced by the mean value of the third principal component, which is 2.898, nearing 3 (see Table 5). The results, on the other hand, suggest that the respondents were not satisfied with the statement of fourth PC, as its mean value is 2.277, which is less than 3 (see Table 4).

The binary logistic regression results indicate a negative relationship between students' personal cybersecurity activities and their use of unique, strong passwords in their online accounts (p = 0.004). Similarly, a clear negative relationship exists between educational institution's cybersecurity literacy and students' adoption of unique, strong passwords for their online accounts (p < .05) (see Tables 3 and 5).

Discussion, conclusion, and suggestion

Our study indicates that respondents reported inadequate to moderate cybersecurity practices at their corresponding institutions offering bachelor's degrees. Additionally, two PCs for personal use and data/network security have KMO and alpha values that are satisfactory. The results reveal an unexpected negative correlation between personal security practices and cybersecurity literacy in educational institution's, as indicated by the binary outcomes (see Tables 3 and 5). The most important—and perhaps most puzzling—finding is the negative correlation between individuals claiming to be knowledgeable about cybersecurity and actually using unique, strong passwords. Some of these causes are problems with measurement and construct validity: The scales may be measuring what people think they know or how they feel in general, rather than what they actually do. People who think they "know" security can claim to know more than they do and fail to report certain behaviors if the wording of the items is unclear.

The main finding of this study is that Nepalese students with bachelor's degrees have poor to moderate cybersecurity awareness. The low mean scores for the main PCs, including "personal cybersecurity practices" at 2.227 and "data protection and network security" at 2.136 (both below the neutral threshold of 3), lead to this conclusion. Students expressed dissatisfaction with remarks on basic safety routines, such as enabling two-factor authentication (2FA) for essential accounts, being cautious about clicking on unfamiliar links, and regularly updating their privacy settings. This aligns with the global environment, which consistently shows that students lack a sufficient understanding of cybersecurity and are unaware of common cyber threats.

The binary logistic regression analysis revealed a statistically significant and negative association between both "personal cybersecurity practices" and "university cybersecurity literacy" and the actual use of unique, strong passwords (p = .014 and p = .004, respectively). This study supports the concept in the literature about the "discrepancy between awareness and action," which suggests that people are aware of threats but do not take steps to protect themselves. The study also indicates a deficiency in formal education, as respondents expressed dissatisfaction with the "mandatory cybersecurity education" component (mean 2.277) and revealed uncertainty regarding their university's provision of guidelines or dedicated cybersecurity modules, thereby corroborating the literature that educational institutions have an insufficient curriculum.

This study's limitations

Methodological Limitation (One Way): The research employed a unique quantitative method (survey methodology), relying on a single data gathering technique, which may not provide a comprehensive understanding of the subject compared to a mixed-methods approach.

Design Limitation (Cross-Sectional): The study relies on a single survey conducted at a specific point in time (cross-sectional), which limits the ability to track temporal variations or demonstrate shifts in awareness resulting from training or educational initiatives.

Validity Limitation (Measurement Issues): The unforeseen adverse connection between reported literacy/practices and the utilisation of unique, robust passwords indicates possible measurement challenges or concerns regarding construct validity. The scales might have been evaluating people's beliefs about what they know or how they typically feel, rather than what they actually do.

Scope Limitation (Surface-Level Behaviour): The study primarily examines surface-level awareness and does not delve into the numerous elements that influence how students actually respond in real-life digital situations.

Evaluation Limitation: The study did not assess the efficacy of current cybersecurity education and curriculum; it merely validated the absence of specialized modules and student discontent with present educational initiatives.

Contextual Limitation: The study is conducted in an environment characterized by a significant scarcity of research exploring profound themes in cybersecurity, particularly within the Nepalese context, which constrains the capacity to derive more nuanced comparison results.

References

Adhikari, B. P. (2022). An investigation into the impact of key components of the induction program on the retention of new teachers in Chitwan District, Nepal. In Erepo.uef.fi. Itä-Suomen Yliopisto. https://erepo.uef.fi/items/714c6a5f-1ad1-4e05-b7e2-7dadd693ab77.

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.

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.

Ahmed, A. A., & Ahmed, W. A. (2019). An Effective Multifactor Authentication Mechanism Based on Combiners of Hash Function over Internet of Things. *Sensors, 19*(17), 3663. https://doi.org/10.3390/s19173663.

Ahmed, O. S. (2021). Teacher's awareness to develop student cyber security: A Case Study. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12*(10), 5148-5156.

Ajzen, I.(1991). The theory of planned behavior organizational behavior and human decision processes, 50(2), 179-211.

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing, 5*(2), 23.

Aljohni, W., Elfadil, N., Jarajreh, M., & Gasmelsied, M. (2021). Cybersecurity Awareness Level: The Case of Saudi Arabia University Students. *International Journal of Advanced Computer Science and Applications (IJACSA), 12*(3), 263–274.

Althobaiti, M. M. (2021). Assessing User's Susceptibility and Awareness of Cybersecurity Threats. *Intelligent Automation & Soft Computing, 28*(1), 167–177. https://doi.org/10.32604/iasc.2021.016660

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1).

Bada, M., Van Den Hoven, J., & Von Solms, R. (2019). Towards a framework for evaluating cybersecurity awareness campaigns in African nations. *Journal of Cyber Policy, 4*(2), 164–181.

Basit, A., Waheed, V. O. O., & Oguntayo, O. O. (2025). The relationship between cybersecurity awareness and secretaries' job performance in University of Ibadan. *International Journal of Science and Research Archive, 16*(1), 662–674. https://doi.org/10.30574/ijsra.2025.16.1.2068

Bhandari, B. (2025). Cybersecurity Awareness amongst University Students: Legal Remedies and Policies to Mitigate Risks. *Unity Journal, 6*(1), 120-135.

Chandarman, R., & Van Niekerk, J. (2017). An assessment of cybersecurity awareness among students at a private tertiary education institution in South Africa. *South African Journal of Information Management, 19*(1), a765.

Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). SAGE Publications.

Djeki, E., Dégila, J., & Alhassan, M. H. (2024). West African online learning spaces security status and students' cybersecurity awareness level during COVID-19 lockdown. *Education and Information Technologies, 29*(12), 15557–15587.

Eliza, F., Fadli, R., Ramadhan, M. A., Sutrisno, V. L. P., Hidayah, Y., Hakiki, M., & Dermawan, D. D. (2024). Assessing student readiness for mobile learning from a cybersecurity perspective. *Online Journal of Communication and Media Technologies, 14*(4), e202452.

Elradi, H. A., Musa, H. O., & Babiker, A. H. (2020). Assessment of cybersecurity awareness and user compliance among university students and staff in Sudan. *International Journal of Engineering Research and Technology, 9*(10), 45–51.

Garba, A. A., Siraj, M. M., & Othman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. *International Journal of Electrical and Computer Engineering (IJECE), 12*(1), 572-584.

Garba, A., Mohammed, I. K., & Yakubu, A. (2020). Cybersecurity awareness among computer science students in Yobe State University, Nigeria. *International Journal of Advanced Research in Computer Science and Software Engineering, 10*(5), 14–22.

Giri, S. (2021). Online Education in Nepal: Prospects and Challenges. *International Journal of Science and Research, 10*(6). https://doi.org/10.21275/SR21318103310.

Gupta, L., & Misra, D. C. (2025). The Impact of Data-Driven Approaches on Cyber Security Awareness in Nepal's Digital Landscape. Aadim Journal of Multidisciplinary Research Information & Technology, 1.

Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N. L., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Education and information technologies, 28*(1), 439-470.

https://doi.org/10.3390/f2040948.

Indian Emblem Government of India Press Information Bureau. (2017). DARPG issues the guidelines for the 28th National e-Governance Awards Scheme 2025. Pib.gov.in. https://www.pib.gov.in/PressReleseDetail.aspx?PRID=2089423®=3&lang

Ismailova, A., & Muhametjanova, G. (2016). Investigation of the relationship between information security awareness, computer literacy, and students' academic fields. In Proceedings of the 13th International Conference on Information Technology and Management.

Kalame, F. B., Luukkanen, O., & Kanninen, M. (2011). Making the National Adaptation Programme of Action (NAPA) more responsive to the livelihood needs of tree planting farmers, drawing on previous experience in dryland Sudan. *Forests, 2*(4), 948-960.

Lohani, A., & Kumar, E. (2024). Impact of Cyber Security Awareness Among Higher Studies: Case Study of Nepal. *LBEF Research Journal of Science, 72*. https://www.lbef.org/journal/6-1/download/6-1-72-81.pdf

Lund, B. D., Anderson, B., Roeschley, A., & Hossain, G. (2025). Understanding the relationship between personal data privacy literacy and data privacy information sharing by university students. Journal of Information Science.

Moyo, M., Loock, M., Sadeck, O., Tunjera, N., & Chigona, A. (2022). Investigating Cyber Security Awareness Among Preservice Teachers During the COVID-19 Pandemic. In R. F. S. W. M. V. (Eds.), Lecture Notes in Business Information Processing: Information and Communication Technology and Society (pp. 53–71). Springer.

National e-Governance Awards Scheme. https://vajiramandravi.com/upsc-daily-current-affairs/prelims-pointers/national-e-governance-awards-scheme/

Nepal, S. (2025). The Impact of Data-Driven Approaches on Cyber Security Awareness in Nepal's Digital Landscape.

Rogers, E. M. (1962). Diffusion of Innovations. Free Press, New York.

Sarathchandra, D., Aladag, A., & O'Leary, J. (2016). Cybersecurity awareness, perceptions, and practices of college students. *Journal of Homeland Security and Emergency Management, 13*(4), 513–536.

Schrieks, T., Botzen, W. J. W., Wens, M., Haer, T.,

& Aerts, J. C. J. H. (2021). Integrating Behavioral Theories in Agent-Based Models for Agricultural Drought Risk Assessments. Frontiers in Water, 3. https://doi.org/10.3389/frwa.2021.686329.

Shahbazi, Z., Jalali, R., & Molaeevand, M. (2025). AI-Based Phishing Detection and Student Cybersecurity Awareness in the Digital Age. *Big Data and Cognitive Computing, 9*(8), 210. https://doi.org/10.3390/bdcc9080210

Szumski, O. (2018). Cybersecurity best practices among Polish students. Procedia Computer Science, 126, 1271-1280.

Talpe, G. (2023). Cyber security among college students. Department of Computer Science..

Tirumala, R., Deakin, E., & Stannard, L. (2016). Internet and cybersecurity awareness among students in Auckland, New Zealand. J*ournal of Applied Computing and Information Technology, 20*(2), 1–10.

Yadav, A. K. (2024). A STUDY ON THE ADEQUACY AND APPROPRIATENESS OF COMPUTER SCIENCE CURRICULA IN NEPALI SECONDARY SCHOOLS (Doctoral dissertation, Tribhuvan University Kathmandu).

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems, 62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269